

**Boost Aerospace**  
**Bridge Certificate Policy**

*Version: 1.1*

*Effective Date: 22 March 2011*

## Signature Page

Validation has been made during BoostAeroSpace Security Management Authority Meeting of 22/03/2011 by:

EADS PKI representative: Romain BOTTAN

Dassault PKI representative: Thierry CHENU

Safran PKI representative: Valérie LEVACQUE

Thales PKI representative: Bernard DENIS

\_\_\_\_\_  
Boost Aerospace Policy Management Authority

22/03/2011  
Date

1. INTRODUCTION .....	10
1.1 Overview .....	10
1.1.1 Certificate Policy .....	10
1.1.2 Relationship between this CP and the Boost Bridge CPS and Boost Root CPS .....	11
1.1.3 Relationship between this CP and the Principal CA CP .....	11
1.1.4 Scope .....	11
1.2 Document Name and Identification .....	12
1.3 PKI Participants .....	12
1.3.1 PKI Authorities .....	12
1.3.2 Registration Authorities .....	13
1.3.3 Subscribers .....	13
1.3.4 Relying Parties .....	13
1.3.5 Other Participants .....	14
1.3.6 Applicability .....	14
1.4 Certificate Usage .....	14
1.4.1 Appropriate Certificate Uses .....	14
1.4.2 Prohibited Certificate Uses .....	14
1.5. Policy Administration .....	14
1.5.1 Organization administering the document .....	14
1.5.2 Contact Person .....	14
1.5.3 Person Determining Certificate Practice Statement Suitability for the Policy .....	14
1.5.4. CPS Approval Procedures .....	15
1.5.5. Waivers .....	15
1.6. Definitions and Acronyms .....	15
2. PUBLICATION AND PKI REPOSITORY RESPONSIBILITIES .....	23
2.1 PKI Repositories .....	23
2.2 Publication of Certificate Information .....	23
2.2.1 Publication of CA Information .....	23
2.2.2 Interoperability .....	23
2.3 Time or Frequency of Publication .....	24
2.4 Access Controls on PKI Repositories .....	25
3 Identification and Authentication .....	26
3.1. Naming .....	26
3.1.1 Types of Names .....	26
3.1.2 Need for Names to be Meaningful .....	26
3.1.3 Anonymity or Pseudonymity of Subscribers .....	26
3.1.4 Rules for Interpreting Various Name Forms .....	26
3.1.5 Uniqueness of Names .....	26
3.1.6 Recognition, Authentication and Role of Trademarks .....	27
3.2. Initial Identity Validation .....	27
3.2.1 Method to Prove Possession of Private Key .....	27
3.2.2 Authentication of Organization Identity .....	28
3.2.3 Authentication of Individual Identity .....	28
3.2.4 Authentication of Component Identity .....	30
3.2.5 Non-verified Subscriber Information .....	31
3.2.6 Validation of Authority .....	31

3.2.7	Criteria for Interoperation .....	31
3.3	Identification and Authentication for Re-Key Requests .....	32
3.3.1	Identification and Authentication for Routine Re-key .....	32
3.3.2	Identification and Authentication for Re-key after Revocation .....	32
3.4.	Identification and Authentication for Revocation Requests .....	32
4	CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS .....	33
4.1	Certificate Application .....	33
4.1.1	Submission of Certificate Application .....	33
4.1.2	Enrollment Process and Responsibilities .....	33
4.2	Certificate Application Processing .....	34
4.2.1	Performing Identification and Authentication Functions .....	34
4.2.2	Approval or Rejection of Certificate Applications .....	34
4.2.3	Time to Process Certificate Applications .....	34
4.3	Certificate Issuance .....	34
4.3.1	CA Actions during Certificate Issuance .....	35
4.3.2	Notification to Subscriber of Certificate Issuance .....	35
4.4	Certificate Acceptance .....	35
4.4.1	Conduct Constituting Certificate Acceptance .....	35
4.4.2	Publication of the Certificate by the CA .....	35
4.4.3	Notification of Certificate Issuance by the CA to Other Entities .....	35
4.5	Key Pair and Certificate Usage .....	36
4.5.1	Subscriber Private Key and Certificate Usage .....	36
4.5.2	Relying Party Public Key and Certificate Usage .....	36
4.6	Certificate Renewal .....	36
4.6.1	Circumstance for Certificate Renewal .....	36
4.6.2	Who may Request Renewal .....	36
4.6.3	Processing Certificate Renewal Requests .....	37
4.6.4	Notification of New Certificate Issuance to Subscriber .....	37
4.6.5	Conduct Constituting Acceptance of a Renewal Certificate .....	37
4.6.6	Publication of the Renewal Certificate by the CA .....	37
4.6.7	Notification of Certificate Issuance by the CA to Other Entities .....	37
4.7	Certificate Re-Key .....	37
4.7.1	Circumstance for Certificate Re-key .....	37
4.7.2	Who may Request Certification of a New Public Key .....	37
4.7.3	Processing Certificate Re-keying Requests .....	37
4.7.4	Notification of New Certificate Issuance to Subscriber .....	38
4.7.5	Conduct Constituting Acceptance of a Re-keyed Certificate .....	38
4.7.6	Publication of the Re-keyed Certificate by the CA .....	38
4.7.7	Notification of Certificate Issuance by the CA to Other Entities .....	38
4.8	Certificate Modification .....	38
4.8.1	Circumstance for Certificate Modification .....	38
4.8.2	Who may Request Certificate Modification .....	38
4.8.3	Processing Certificate Modification Requests .....	38
4.8.4	Notification of New Certificate Issuance to Subscriber .....	38
4.8.5	Conduct Constituting Acceptance of Modified Certificate .....	38
4.8.6	Publication of the Modified Certificate by the CA .....	38
4.8.7	Notification of Certificate Issuance by the CA to Other Entities .....	39
4.9	Certificate Revocation and Suspension .....	39
4.9.1	Circumstance for Revocation of a Certificate .....	39

4.9.2	Who Can Request Revocation of a Certificate .....	39
4.9.3	Procedure for Revocation Request .....	39
4.9.4	Revocation Request Grace Period .....	40
4.9.5	Time within which CA must Process the Revocation Request .....	40
4.9.6	Revocation Checking Requirements for Relying Parties .....	41
4.9.7	CRL Issuance Frequency .....	41
4.9.8	Maximum Latency for CRLs.....	41
4.9.9	Online Revocation Checking Availability .....	42
4.9.10	Online Revocation Checking Requirements.....	42
4.9.11	Other Forms of Revocation Advertisements Available .....	42
4.9.12	Special Requirements Related To Key Compromise.....	42
4.9.13	Circumstances for Suspension.....	42
4.9.14	Who can Request Suspension.....	42
4.9.15	Procedure for Suspension Request.....	42
4.9.16	Limits on Suspension Period.....	42
4.10	Certificate Status Services .....	42
4.10.1	Operational Characteristics .....	42
4.10.2	Service Availability.....	43
4.10.3	Optional Features .....	43
4.11	End Of Subscription .....	43
4.12	Key Escrow and Recovery.....	43
4.12.1	Key Escrow and Recovery Policy and Practices.....	43
4.12.2	Session Key Encapsulation and Recovery Policy and Practices.....	43
5	FACILITY MANAGEMENT & OPERATIONAL CONTROLS.....	44
5.1	Physical Controls .....	44
5.1.1	Site Location & Construction .....	44
5.1.2	Physical Access .....	44
5.1.3	Power and Air Conditioning.....	45
5.1.4	Water Exposures .....	45
5.1.5	Fire Prevention & Protection .....	45
5.1.6	Media Storage.....	45
5.1.7	Waste Disposal .....	45
5.1.8	Off-Site backup.....	46
5.2	Procedural Controls.....	46
5.2.1	Trusted Roles.....	46
5.2.2	Number of Persons Required per Task .....	48
5.2.3	Identification and Authentication for Each Role.....	49
5.2.4	Roles Requiring Separation of Duties .....	49
5.3	Personnel Controls .....	49
5.3.1	Qualifications, Experience, and Clearance Requirements.....	49
5.3.2	Background Check Procedures .....	50
5.3.3	Training Requirements .....	51
5.3.4	Retraining Frequency and Requirements.....	51
5.3.5	Job Rotation Frequency and Sequence .....	51
5.3.6	Sanctions for Unauthorized Actions.....	51
5.3.7	Independent Contractor Requirements.....	51
5.3.8	Documentation Supplied To Personnel.....	51
5.4	Audit Logging Procedures.....	52
5.4.1	Types of Events Recorded.....	52

5.4.2	Frequency of Processing Audit Logs .....	55
5.4.3	Retention Period for Audit Logs .....	55
5.4.4	Protection of Audit Logs .....	55
5.4.5	Audit Log Backup Procedures .....	56
5.4.6	Audit Collection System (internal vs. external) .....	56
5.4.7	Notification to Event-Causing Subject .....	56
5.4.8	Vulnerability Assessments .....	56
5.5	Records Archival .....	56
5.5.1	Types of Records Archived .....	56
5.5.2	Retention Period for Archive .....	57
5.5.3	Protection of Archive.....	57
5.5.4	Archive Backup Procedures.....	57
5.5.5	Requirements for Time-Stamping of Records .....	58
5.5.6	Archive Collection System (internal or external) .....	58
5.5.7	Procedures to Obtain & Verify Archive Information.....	58
5.6	Key Changeover .....	58
5.7	Compromise and Disaster Recovery .....	59
5.7.1	Incident and Compromise Handling Procedures .....	59
5.7.2	Computing Resources, Software, and/or Data are Corrupted.....	59
5.7.3	Private Key Compromise Procedures .....	60
5.7.4	Business Continuity Capabilities after a Disaster.....	61
5.8	CA, CSA, and RA Termination .....	61
6	TECHNICAL SECURITY CONTROLS .....	62
6.1	Key Pair Generation and Installation.....	62
6.1.1	Key Pair Generation .....	62
6.1.2	Private Key Delivery to Subscriber .....	63
6.1.3	Public Key Delivery to Certificate Issuer .....	64
6.1.4	CA Public Key Delivery to Relying Parties.....	64
6.1.5	Key Sizes .....	64
6.1.6	Public Key Parameters Generation and Quality Checking.....	65
6.1.7	Key Usage Purposes (as per X.509 v3 key usage field).....	65
6.2	Private Key Protection and Cryptographic Module Engineering Controls .....	65
6.2.1	Cryptographic Module Standards and Controls .....	65
6.2.2	Private Key Multi-Person Control .....	66
6.2.3	Private Key Escrow .....	66
6.2.4	Private Key Backup.....	66
6.2.5	Private Key Archival.....	67
6.2.6	Private Key Transfer into or from a Cryptographic Module .....	67
6.2.7	Private Key Storage on Cryptographic Module .....	67
6.2.8	Method of Activating Private Key .....	67
6.2.9	Methods of Deactivating Private Key .....	67
6.2.10	Method of Destroying Private Key .....	67
6.2.11	Cryptographic Module Rating .....	67
6.3	Other Aspects of Key Management .....	68
6.3.1	Public Key Archival .....	68
6.3.2	Certificate Operational Periods/Key Usage Periods .....	68
6.4	Activation Data .....	68
6.4.1	Activation Data Generation and Installation .....	68
6.4.2	Activation Data Protection .....	68

6.4.3	Other Aspects of Activation Data .....	68
6.5	Computer Security Controls .....	68
6.5.1	Specific Computer Security Technical Requirements .....	68
6.5.2	Computer Security Rating.....	69
6.6	Life-Cycle Technical Controls .....	69
6.6.1	System Development Controls .....	69
6.6.2	Security Management Controls.....	70
6.6.3	Life Cycle Security Controls .....	70
6.7	Network Security Controls.....	70
6.8	Time Stamping .....	70
7	CERTIFICATE, CRL, AND OCSP PROFILES .....	72
7.1	Certificate Profile .....	72
7.1.1	Version Numbers.....	72
7.1.2	Certificate Extensions .....	72
7.1.3	Algorithm Object Identifiers.....	72
7.1.4	Name Forms .....	72
7.1.5	Name Constraints.....	74
7.1.6	Certificate Policy Object Identifier.....	74
7.1.7	Usage of Policy Constraints Extension .....	74
7.1.8	Policy Qualifiers Syntax and Semantics .....	75
7.1.9	Processing Semantics for the Critical Certificate Policy Extension....	75
7.2	CRL Profile .....	75
7.2.1	Version Numbers.....	75
7.2.2	CRL and CRL Entry Extensions .....	75
7.3	OCSP Profile.....	75
7.3.1	Version Number .....	75
7.3.2	OCSP Extensions .....	75
8.	Compliance Audit and Other Assessment.....	76
8.1	Frequency or Circumstances of Assessments.....	76
8.2	Identity and Qualifications of Assessor.....	76
8.3	Assessor's Relationship to Assessed Entity .....	76
8.4	Topics Covered by Assessment .....	76
8.5	Actions Taken as a Result of Deficiency .....	76
8.6	Communication of Results.....	77
9	OTHER BUSINESS AND LEGAL MATTERS.....	78
9.1	Fees.....	78
9.1.1	Certificate Issuance and Renewal Fees .....	78
9.1.2	Certificate Access Fees.....	78
9.1.3	Revocation or Status Information Access Fees.....	78
9.1.4	Fees for Other Services .....	78
9.1.5	Refund Policy .....	78
9.2	Financial Responsibility .....	78
9.2.1	Insurance Coverage.....	78
9.2.2	Other Assets.....	78
9.2.3	Insurance or Warranty Coverage for End-Entities .....	78
9.3	Confidentiality of Business Information .....	79
9.4	Privacy of Personal Information .....	79
9.5	Intellectual Property Rights .....	79
9.5.1	Property Rights in Certificates and Revocation Information.....	79

9.5.2	Property Rights in the CPS.....	80
9.5.3	Property Rights in Names .....	80
9.5.4	Property Rights in Keys .....	80
9.6	Representations and Warranties.....	80
9.6.1	CA Representations and Warranties .....	80
9.6.2	Subscriber Agreement .....	81
9.6.3	Relying Party .....	82
9.6.4	Representations and Warranties of Affiliated Organizations.....	82
9.6.5	Representations and Warranties of Other Participants .....	82
9.7	Disclaimers of Warranties.....	82
9.8	Limitations of Liabilities .....	83
9.9	Indemnities.....	84
9.9.1	Indemnification Customer CAs .....	84
9.9.2	Indemnification by Relying Parties.....	84
9.10	Term and Termination.....	85
9.10.1	Term.....	85
9.10.2	Termination .....	85
9.10.3	Effect of Termination and Survival .....	85
9.11	Individual Notices and Communications with Participants.....	85
9.12	Amendments .....	85
9.12.1	Procedure for Amendment .....	85
9.12.2	Notification Mechanism and Period.....	86
9.12.3	Circumstances under Which OID Must be Changed .....	86
9.13	Dispute Resolution Provisions .....	86
9.13.1	Disputes among Boost Aerospace and Customers .....	86
9.13.2	Alternate Dispute Resolution Provisions .....	86
9.14	Governing Law.....	87
9.15	Compliance with Applicable Law.....	87
9.16	Miscellaneous Provisions .....	87
9.16.1	Entire Agreement .....	87
9.16.2	Assignment.....	87
9.16.3	Severability .....	87
9.16.4	Waiver of Rights.....	87
9.16.5	Force Majeure .....	87
9.17	Other Provisions .....	88
10	Certificate Profiles.....	89
10.1	Boost Bridge CA to Principal CA .....	91
10.2	Principal CA to Boost Bridge CA .....	92
10.4	Intermediate or Signing CA Certificate.....	94
10.5	Subscriber Identity Certificate .....	95
10.6	Subscriber Signature Certificate.....	96
10.7	Subscriber Encryption Certificate .....	97
10.9	Code Signing Certificate.....	98
10.10	Device or Server Certificate .....	99
10.11	OCSP Responder Certificate .....	100
10.12	CRL Format .....	101
10.12.1	Full and Complete CRL .....	101
10.12.2	Distribution Point Based Partitioned CRL .....	101
10.13	OCSP Request Format.....	103

10.14 OCSP Response Format.....	103
Appendix A: Bibliography .....	104
Appendix B: Glossary .....	105

# 1. INTRODUCTION

This Certificate Policy is consistent with the Internet Engineering Task Force (IETF) RFC 3647, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Statement Framework".

## 1.1 Overview

This Certificate Policy (CP) defines several assurance levels which may be used by applications and companies within the aerospace and air transport communities to facilitate interoperability between Public Key Infrastructure (PKI) domains. The term "assurance" used in this CP means how confident a Relying Party may be in the identity binding between a public key it is presented, and the individual whose subject name is in the associated X.509 Certificate (Security Principal). In addition, it may also give an indication of how assured a Relying Party may be that the Security Principal truly is in sole possession of the corresponding private key, as well as how secure the system was that was used to produce the Certificate.

Boost Aerospace intends to operate a Bridge Certification Authority based on this policy to facilitate interoperability at a technical level among aerospace PKIs. Such PKIs will be required to comply with all aspects of this CP, as demonstrated through the use of policy mapping between such a PKI's CP and this CP.

Any use of this CP outside of the scope hereabove mentioned is entirely at the using party's risk. No Entity shall assert any OID listed in section 1.2 of this CP, unless that party has been granted permission in writing to do so by Boost Aerospace, and, in such a case, said Entity shall only assert the OIDs in the policyMappings X.509 extension of a Cross-Certificate issued according to the profile in section 10.2, and in accordance with a duly completed policy mapping between the Boost Aerospace OID, and an OID in the Entities PKI CP, as deemed appropriate by a duly appointed representative of Boost Aerospace.

### 1.1.1 Certificate Policy

All X.509 Certificates, except Trust Anchor Certificates, issued under this Certificate Policy must contain one or more registered Certificate Policy Object Identifiers (OID), each of which is associated with a given assurance level as indicated in section 1.2 of this CP. The same Entity that is described by the OID also publishes the corresponding CP, and Relying Parties may use this CP to establish if a given Certificate satisfies their requirements for identity assurance.

Cross-Certificates issued by the Boost Aerospace Bridge CA shall, in the policyMappings X.509 extension, reflect what mappings exist between this CP and the cross-certified Entities CP.

### **1.1.2 Relationship between this CP and the Boost Bridge CPS and Boost Root CPS**

This CP states what assurance can be placed in a Certificate issued under this policy. The Boost Bridge CA Certification Practice Statement (CPS) and Boost Root CA CPS state how the respective certification authorities establish that assurance.

### **1.1.3 Relationship between this CP and the Principal CA CP**

During the process of becoming cross-certified with the Boost Aerospace Bridge CA, an Entity's CP is examined, and, if possible, equivalence is established between the assurance levels outlined in the Entity's CP and this CP. Once equivalence is established, the Boost Policy Management Authority (PMA) causes the Boost Operational Authority (OA) to issue a Cross-Certificate according to the profile in section 10.1, which will contain in it, the appropriate policy mappings. The OA may also publish this information in any other ways that would facilitate interoperability.

### **1.1.4 Scope**

This CP imposes requirements on:

- The Boost Aerospace Bridge CA (BBCA); and
- Any CA that is cross-certified with the BBCA; and
- Other bridge CAs with whom the BBCA cross-certifies; and
- Any Root CAs, Intermediate CAs, or Signing CAs that are within a policy domain cross-certifying with the BBCA and which operate at an assurance level that is cross-certified with the BBCA.

The BBCA shall only issue Certificates to:

- Other CAs and Bridge CAs upon completion of a successful policy mapping, and approval by the Boost Policy Management Authority; and
- Individuals who operate the BBCA, in strict measure with operational necessity.

The scope of this CP, in terms of Subscriber Certificate types is limited to those listed in Section 10, and repeated here:

1. Identity
2. Signature
3. Encryption
4. Device
5. Code Signing
6. Role Signature
7. Role Encryption

## 1.2 Document Name and Identification

This CP identifies 3 levels of assurance which are further described in the rest of this document. Each assurance level has a distinct OID, which is asserted in the CertificatePolicies X.509 extension of a Certificate which is issued in a manner that complies with the requirements herein for that assurance level.

These OIDS are as follows:

id-boost	::= { <b>FIXME</b> }
id-pki	::= { id-boost 1 }
id-Certificate-policies	::= { id-pki 1 }
id-basic	::= { id-Certificate-policies 1 }
id-medium-sw	::= { id-Certificate-policies 2 }
id-medium-hw	::= { id-Certificate-policies 3 }

## 1.3 PKI Participants

### 1.3.1 PKI Authorities

#### 1.3.1.1 Boost Aerospace PMA (BPMA)

The BPMA is responsible for:

- Drafting and approval of this CP; and
- Drafting, compliance analysis, and approval of the BBKA CPS; and
- Accepting and processing applications from Entities desiring to cross-certify with the BBKA; and
- Determining the mappings between Certificates issued by applicant Entity CAs and the levels of assurance set forth in the BBKA CP (which will include objective and subjective evaluation of the respective CP contents and any other facts deemed relevant by the BPMA); and
- After an Entity is authorized to interoperate using the BBKA, ensuring continued conformance of that Entity with applicable requirements as a condition for allowing continued interoperability using the BBKA.

A complete description of BPMA roles and responsibilities are provided in the BPMA Charter [CHARTER].

Boost Aerospace will enter into a Memorandum of Agreement (MOA) with an Entity setting forth the respective responsibilities and obligations of both parties, and the mappings between the Certificate levels of assurance contained in this CP and those in the Entity CP. Boost Aerospace will consult the BPMA chair prior to entering into a MOA. Thus, the term "MOA" as used in this CP shall always refer to the Memorandum of Agreement cited in this paragraph.

#### 1.3.1.2 Boost Operational Authority

### **1.3.1.3 Boost Operational Authority Administrator**

### **1.3.1.4 Boost Operational Authority Officers**

### **1.3.1.5 Entity Principal Certification Authority (PCA)**

The Principal CA is a CA within a PKI that has been designated to interoperate directly with the BBCCA (e.g., through the exchange of Cross-Certificates). It should be noted that an Entity may request that the BBCCA inter-operate with more than one CA within the Entity; that is, an Entity may have more than one Principal CA. A PCA may or may not be a Root CA (trust anchor) for its PKI Enterprise.

### **1.3.1.6 Root CA**

A Root CA is CA which is characterised by having itself as the issuer (that is, it is self signed). Root CAs may not be revoked in the normal manner (they are not put on an Authority Revocation List), and, when used as a Trust Anchor, must be securely transmitted to any Relying Parties which choose to accept it as one by the mechanisms outlined in section 6.1.4.

Normally, the PCA is also the Root CA. However, in some situations, a Root CA may not be a PCA.

### **1.3.1.7 Intermediate CA**

An Intermediate CA is a CA that is not a Root CA and whose primary function is to issue Certificates to other CAs. Intermediate CAs may or may not issue some end entity Certificates.

### **1.3.1.8 Signing CA**

A Signing CA is a CA whose primary function is to issue Certificates to the end entities. A Signing CA does not issue Certificates to other CAs.

### **1.3.1.9 Boost Bridge Certification Authority (BBCCA)**

The Boost Bridge Certification Authority is a Root CA whose sole purpose is the signature and exchange of Cross-Certificates with Entity PCAs.

The only End-Entity Certificates signed by the BBCCA are Device Certificates used for the BBCCA's operation.

### **1.3.1.10 Certificate Status Authorities**

## **1.3.2 Registration Authorities**

### **1.3.3 Subscribers**

### **1.3.4 Relying Parties**

A Relying Party is 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.

### **1.3.5 Other Participants**

### **1.3.6 Applicability**

## **1.4 Certificate Usage**

### **1.4.1 Appropriate Certificate Uses**

No Stipulation

### **1.4.2 Prohibited Certificate Uses**

No Stipulation

## **1.5. Policy Administration**

### **1.5.1 Organization administering the document**

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

### **1.5.2 Contact Person**

Questions regarding this CP shall be directed to the Chair of the Boost PMA. Current contact details for the chair may be found at:

**FIXME – ADD URL**

### **1.5.3 Person Determining Certificate Practice Statement Suitability for the Policy**

The term CPS is defined in the [RFC 3647] as: "A statement of the practices, which a Certification Authority employs in issuing Certificates." It is a comprehensive description of such details as the precise implementation of service offerings and detailed procedures of Certificate life-cycle management. It shall be more detailed than the corresponding Certificate Policy defined above.

A CPS may be approved as sufficient for fulfilling the obligations under this CP when such a CPS has been reviewed by an auditor or compliance analyst competent in the operations of a PKI, and when said person determines that the CPS is in fact in compliance with all aspects of this CP. The auditor or compliance analyst shall be from a firm which is independent from the entity being audited. Additionally, the auditor or compliance analyst may not be the author of the subject CPS.

For the CBCA, the Boost PMA shall approve the Boost Bridge CPS, and shall furthermore make the determination whether a compliance analyst meets the requirements outlined herein.

#### 1.5.4. CPS Approval Procedures

The Boost PMA Charter shall outline the specific procedures necessary to approve the Boost Bridge CPS.

Entity PKI PMA's must provide a detailed procedure outlining how a given CPS is approved as valid and compliant to their CP.

#### 1.5.5. Waivers

There shall be no waivers to this CP.

### 1.6. Definitions and Acronyms

Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.
Activation Data	Secret data (e.g.: password, PIN code) that is used to perform cryptographic operations using a Private Key.
Assurance Level	A representation of how well a Relying Party can be certain of the identity binding between the Public Key and the individual whose subject name is cited in the Certificate. In addition, it also reflects how well the Relying Party can be certain that the End-Entity whose subject name is cited in the Certificate is controlling the use of the Private Key that corresponds to the Public Key in the Certificate, and how securely the system which was used to produce the Certificate and (if appropriate) deliver the Private Key to the End-Entity performs its task.
Authority Revocation List (ARL)	A list of revoked Certification Authority Certificates. Technically, an ARL is a CRL.
Authentication	The process whereby one party has presented an identity and claims to be that identity and the second party confirms that this assertion of identity is true.
Audit	An Independent review and examination of documentation, records and activities to 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.
Certificate	A Certificate is a data structure that is digitally signed by a Certification Authority, and that contains the following pieces of information:

	<p>The identity of the Certification Authority issuing it.</p> <p>The identity of the certified End-Entity.</p> <p>A Public Key that corresponds to a Private Key under the control of the certified End-Entity.</p> <p>The Operational Period.</p> <p>A serial number.</p> <p>The Certificate format is in accordance with ITU-T Recommendation X.509 version 3.</p>
Certification Authority (CA)	<p>A Certification Authority is an entity that is responsible for authorising and causing the issuance or revocation of a Certificate.</p> <p>By extension, the term "CA" can also be used to designate the infrastructure component that technically signs the Certificates and the revocation lists it issues.</p> <p>A Certification Authority can perform the functions of a Registration Authority (RA) and can delegate or outsource this function to separate entities.</p> <p>A Certification Authority performs three essential functions. First, it is responsible for identifying and authenticating the intended Authorised Subscriber to be named in a Certificate, and verifying that such Authorised Subscriber possesses the Private Key that corresponds to the Public Key that will be listed in the Certificate. Second, the Certification Authority actually creates and digitally signs the Authorised Subscriber's Certificate. The Certificate issued by the Certification Authority then represents that CA's statement as to the identity of the person named in the Certificate and the binding of that person to a particular public-private Key Pair. Third, the Certification Authority creates and digitally signs the Certificate Revocation Lists and/or Authority Revocation Lists.</p>
Certificate Extension	<p>A Certificate may include extension fields to convey additional information about the associated Public Key, the Subscriber, the Certificate Issuer, or elements of the certification process.</p>
Certificate Manufacturing	<p>The process of accepting a Public Key and identifying information from an authorised Subscriber, producing a digital Certificate containing that and other pertinent information, and digitally signing the Certificate.</p>

Certificate Policy (CP)	<p>A named set of rules that indicates the applicability of a Certificate to a particular community and/or class of applications with common security requirements.</p> <p>Within this document, the term CP, when used without qualifier, refers to the Boost Aerospace CP, as defined in section 1.</p>
Certification Practice Statement (CPS)	<p>A statement of the practices, which a CA employs in issuing and revoking Certificates, and providing access to same. The CPS defines the equipment and procedures the CA uses to satisfy the requirements specified in the CP that are supported by it.</p>
Certificate Request	<p>A message sent from an applicant to a CA in order to apply for a digital Certificate. The Certificate request contains information identifying the applicant and the Public Key chosen by the applicant. The corresponding Private Key is not included in the request, but is used to digitally sign the entire request.</p> <p>If the request is successful, the CA will send back a Certificate that has been digitally signed with the CA's Private Key.</p>
Certificate Revocation List (CRL)	<p>A list of revoked Certificates that is created, time stamped and signed by a CA. A Certificate is added to the list if revoked (e.g., because of suspected key compromise, distinguished name (DN) change) and then removed from it when it reaches the end of the Certificate's validity period. In some cases, the CA may choose to split a CRL into a series of smaller CRLs.</p> <p>When an End-Entity chooses to accept a Certificate the Relying Party Agreement requires that this Relying Party check that the Certificate is not listed on the most recently issued CRL.</p>
Certificate Status Authority (CSA)	<p>A CSA is an authority that provides status of Certificates or certification paths.</p>
Common Criteria	<p>Common Criteria for Information Technology Security Evaluation is an international standard (ISO/IEC 15408) for information technology security certification.</p>
Cross-Certificate (CC)	<p>A Certificate used to establish a trust relationship between two Certification Authorities.</p> <p>A Cross-Certificate is a Certificate issued by one CA to another CA which contains the subject CA Public Key associated with the private CA signature key used by the subject CA for issuing Certificates. Typically a Cross-Certificate is used to allow End-Entities in one CA</p>

	domain to communicate securely with End-Entities in another CA domain. A Cross-Certificate issued by CA#1 to CA#2 allows Entity #a, who has a Certificate issued by CA#1 domain, to accept a Certificate used by Entity #b, who has a Certificate issued to Entity #b by CA#2.
Digital Signature	<p>The result of a transformation of a message by means of a cryptographic system using keys such that a person who has received a digitally signed message can determine:</p> <p>Whether the transformation was created using the private signing key that corresponds to the signer's public verification key.</p> <p>Whether the message has been altered since the transformation was made.</p>
Distinguished Name	A string created during the certification process and included in the Certificate that uniquely identifies the End-Entity within the CA domain.
Encryption Key Pair	A public and private Key Pair issued for the purposes of encrypting and decrypting data.
Directory	A directory system that conforms to the ITU-T X.500 series of Recommendations.
End-Entity EE	A person, device or application that is issued a Certificate by a CA.
Entity	Any autonomous element within the PKI, including CAs, RAs and End-Entities.
Federal Information Processing Standards (FIPS)	Federal standards that prescribe specific performance requirements, practices, formats, communications protocols, etc. for hardware, software, data, telecommunications operation, etc. U.S. Federal agencies are expected to apply these standards as specified unless a waiver has been granted in accordance with agency waiver procedures.
Hardware Token	A hardware device that can hold Private Keys, digital Certificates, or other electronic information that can be used for authentication or authorisation. Smartcards and USB tokens are examples of hardware tokens.
Hardware Security Module (HSM)	An HSM is a hardware device used to generate cryptographic Key Pairs, keep the Private Key secure and generate digital signatures. It is used to secure the CA keys, and in some cases the keys of some applications (End-Entities).
Internet Engineering Task	The Internet Engineering Task Force is a large open international community of network designers,

Force(IETF)	operators, vendors, and researches concerned with the evolution of the Internet architecture and the smooth operation of the Internet.
Issuing CA	In the context of a particular Certificate, the issuing Certification Authority is the Certification Authority that signed and issued the Certificate.
Key Generation	The process of creating a Private Key and Public Key pair.
Key Pair	Two mathematically related keys, having the properties that (i) one key can be used to encrypt data that can only be decrypted using the other key, and (ii) knowing one of the keys which is called the Public Key, it is computationally infeasible to discover the other key which is called the Private Key.
Local Registration Authority (LRA)	An entity that is responsible for identification and authentication of Certificate subjects, but that does not sign or issue Certificates (i.e., an LRA is delegated certain tasks on behalf of a RA or CA).
Memorandum of Agreement	As used in the context of this CP, between Boost Aerospace and an Entity PKI Domains legal Representation allowing interoperation between the respective Entity PCA and the Boost Bridge CA.
OCSP	Protocol useful in determining the current status of a digital Certificate without requiring CRLs.
Object Identifier (OID)	An object identifier is a specially-formatted sequence of numbers that is registered with an internationally-recognised standards organisation.
Boost Operational Authority (OA)	The Boost Operational authority is an organisation selected by Boost Aerospace to operate the BBKA.
Operational Period of a Certificate	The operational period of a Certificate is the period of its validity. It would typically begin on the date the Certificate is issued (or such later date as specified in the Certificate), and end on the date and time it expires as noted in the Certificate or earlier if revoked.
Organisation	Department, agency, partnership, trust, joint venture or other association.
Person	A human being (natural person), corporation, limited liability company, or other judicial entity, or a digital device under the control of another person.
PIN	Personal Identification Number. See activation data for definition
PKI Disclosure Statement	Defined by IETF's RFC 3647 as "An instrument that supplements a CP or CPS by disclosing critical

(PDS)	information about the policies and practices of a CA/PKI. A PDS is a vehicle for disclosing and emphasizing information normally covered in detail by associated CP and/or CPS documents. Consequently, a PDS is not intended to replace a CP or CPS."
PKIX	IETF Working Group chartered to develop technical specifications for PKI components based on X.509 Version 3 Certificates.
Policy	This Certificate Policy.
Policy Management Authority (PMA)	<p>An agent of the Certification Authority. The Policy Management Authority is responsible for:</p> <ul style="list-style-type: none"> <li>Dispute resolution.</li> <li>Selecting and/or defining Certificate Policies, in accordance with the Internet X.509 Public Key Infrastructure (PKIX) Certificate Policy and Certification Practice Framework (RFC 3647), for use in the Certification Authority PKI or organisational enterprise.</li> <li>Approving of any interoperability agreements with external Certification Authorities.</li> <li>Approving practices, which the Certification Authority must follow by reviewing the Certification Practice Statement to ensure consistency with the Certificate Policies.</li> <li>Providing Policy direction to the CA and the Operational Authority.</li> </ul>
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.
Principal CA (PCA)	CA within a PKI that has been designated to interoperate directly with another PKI (e.g., through the exchange of Cross-Certificates with a PCA in another PKI domain).
Private Key	The Private Key of a Key Pair used to perform Public Key cryptography. This key must be kept secret.
Public Key	The Public Key of a Key Pair used to perform Public Key cryptography. The Public Key is made freely available to anyone who requires it. The Public Key is usually provided via a Certificate issued by a Certification

	Authority and is often obtained by accessing a repository.
Public/Private Key Pair	See Key Pair.
Registration	The process whereby a user applies to a Certification Authority for a digital Certificate.
Registration Authority (RA)	An Entity that is responsible for the identification and authentication of Certificate Subscribers before Certificate issuance, but does not actually sign or issue the Certificates (i.e., an RA is delegated certain tasks on behalf of a CA).
Relying Party (RP)	A 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.
Repository	Publication service providing all information necessary to ensure the intended operation of issued digital Certificates (e.g.: CRLs, encryption Certificates, CA Certificates).
Revocation	To prematurely end the Operational Period of a Certificate from a specified time forward.
RFC3647	Document published by the IETF, which presents a framework to assist the writers of Certificate Policies or certification practice statements for participants within Public Key infrastructures, such as certification authorities, policy authorities, and communities of interest that wish to rely on Certificates. In particular, the framework provides a comprehensive list of topics that potentially (at the writer's discretion) need to be covered in a Certificate Policy or a certification practice statement.
Root CA	The CA that is the trust anchor for a set of relying parties.
SCVP	Protocol that allows a client to delegate Certificate path construction and Certificate path validation to a server.
Signature Key Pair	A public and private Key Pair used for the purposes of digitally signing electronic documents and verifying digital signatures.
Software-based Certificate	A digital Certificate (and associated Private Keys) that are created and stored in software – either on a local workstation or on a server.
Sponsoring Organisation	An organisation with which an Authorised Subscriber is affiliated (e.g., as an employee, user of a service, business partner, customer etc.).

Subscriber	An entity that is the subject of a Certificate and which is capable of using, and is authorised to use, the Private Key, that corresponds to the Public Key in the Certificate. Responsibilities and obligations of the Subscriber shall be as required by the Certificate Policy.
Subscriber Agreement	An agreement, entered into by a Subscriber, that provides for the respective liabilities of the Entity PKI and of the Subscriber. Such agreement is a prerequisite in order to be able to use the Private Key associated to the Certificate.
Token	A hardware security device containing an End-Entity's Private Key(s) and Certificate. (see "Hardware Token")
Trusted Agent	An agent who a Registration Authority relies on to verify that an applicant fulfils part of or all of the necessary prerequisites to obtain a Certificate for an End-Entity.
Trustworthy System	Computer hardware, software, and/or procedures that: (a) are reasonably secure from intrusion and misuse; (b) provide a reasonable level of availability, reliability, and correct operation; (c) are reasonably suited to performing their intended functions, and (d) adhere to generally accepted security procedures.
Valid Certificate	A Certificate that (1) a Certification Authority has issued, (2) the Subscriber listed in it has accepted, (3) has not expired, and (4) has not been revoked. Thus, a Certificate is not "valid" until it is both issued by a CA and has been accepted by the Subscriber.

## **2. PUBLICATION AND PKI REPOSITORY RESPONSIBILITIES**

### **2.1 PKI Repositories**

Entities and the Boost Operational Authority may use several methods for posting the artifacts that are required by this CP to an appropriate Repository. However, these mechanisms shall, as a minimum include:

- Directory Server System that is also accessible through the Lightweight Directory Access Protocol (LDAP) or the Hypertext Transport Protocol (HTTP); and
- Availability of the information as required by the Certificate information posting and retrieval stipulations of this CP; and
- Access control mechanisms when needed to protect repository information as described in later sections.

The PKI Repositories containing Certificates and Certificate status information shall be deployed so as to provide 24 hour per day/365 day per year availability at levels of 99.9% availability or better. This requirement does not apply to any PKI component other than the Repositories containing CA signature Certificates and Certificate status information.

### **2.2 Publication of Certificate Information**

#### **2.2.1 Publication of CA Information**

This CP shall be published electronically on the Boost Aerospace web site.

The Boost Operational Authority shall publish any additional information concerning the Boost Bridge CA which is necessary to support its use and operation.

All Entities shall publish:

- All encryption Public Key Certificates issued by Signing CAs to a repository which is, at a minimum, available to all other entities cross-certified with the BBKA; and
- All CRLs, ARLs, CA Certificates, and CA Cross-Certificates publicly to the Internet.

#### **2.2.2 Interoperability**

The following profile shall be used to establish interoperability for PKI repositories:

##### **2.2.2.1 Protocol**

Each Entity shall implement a PKI Repository that provides both LDAP and HTTP protocol access to Certificates and CRLs according to the following:

- Encryption Certificates must be made available, at minimum, using the LDAP protocol; and

- CA, ARL, and CRL information (such as is used by the X.509 authorityInfoAccess and crlDistributionPoint extensions) must be made available, at minimum, using the HTTP protocol.

#### **2.2.2.2 Authentication**

Each PKI Repository shall permit “none” authentication for Relying Parties to read Certificate and CRL information, according to access restrictions allowed by 2.2.1.

Each Enterprise shall be free to implement authentication mechanisms of its choice for browse and list operations.

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

#### **2.2.2.3 Naming**

This CP defines the naming convention to be used for all Issuer, Subject, and SubjectAltName representations.

Certificates shall be stored in the PKI Repository in the entry that appears in the Certificate subject name.

The issuedByThisCA element of crossCertificatePair shall contain the Certificate(s) issued by a CA who name the entry represents.

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

#### **2.2.2.4 Object Class**

Entries that describe CAs shall be a member of pkiCA and cpCPS auxiliary object classes.

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

#### **2.2.2.5 Attributes**

Entries that describe CAs shall be populated with the caCertificate, crossCertificatePair, CertificateRevocationList, and cpCPS attributes, as applicable.

User entries shall be populated with a single userCertificate attribute containing only the currently valid encryption Certificate associated with that User. It shall also be populated with the email address in the “mail” attribute that matches that asserted by the rfc822 email address subjectAltName entry in the Certificate.

### **2.3 Time or Frequency of Publication**

Certificates and Certificate status information shall be published according to the stipulations of section 4 of this CP.

## **2.4 Access Controls on PKI Repositories**

Any PKI Repository information not intended for public dissemination or modification shall be protected. Public keys and Certificate status information in the Boost PKI Repository shall be publicly available through the Internet. Access to information in Entity PKI Repositories shall be determined by the Entity pursuant to the rules and statutes that apply to that entity, but at a minimum, the Entity must publish the information listed as per sections 2.2 of this CP.

## **3 Identification and Authentication**

### **3.1. Naming**

#### **3.1.1 Types of Names**

CAs shall ensure that all Certificates issued have a clearly distinguishable, unique and non-null X.501 Distinguished Name (DN) in the Subject and Issuers fields and in accordance with RFC 5280. Certificates may include additional names via the subjectAltName extension, provided it is marked noncritical, and is in accordance with the profiles in section 10.

#### **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 and associated directory information tree shall accurately reflect organizational structures. When User Principal Name (UPN) is used, it shall accurately reflect organizational structure.

When DNs are used, it is preferable that the common name represents the Subscriber in a way that is easily understandable for humans. For people, this will typically be a legal name. For equipment, this may be a model name and serial number, or an application process (e.g., Organization X Mail List or Organization Y Multifunction Interpreter).

#### **3.1.3 Anonymity or Pseudonymity of Subscribers**

CA Certificates shall not contain anonymous or pseudonymous identities.

DNs in Certificates issued to end entities may contain a pseudonym to meet local privacy regulations as long as name space uniqueness requirements are met and as long as such name is unique and traceable to the actual entity.

#### **3.1.4 Rules for Interpreting Various Name Forms**

Rules for interpreting name forms shall be contained in the applicable Certificate profile. The authority responsible for Entity CA name space control shall be identified in the respective CP.

Rules for interpreting UUID are specified in RFC 4122.

#### **3.1.5 Uniqueness of Names**

Name uniqueness across all of the domains cross-certified with Boost shall be enforced. The CAs and RAs shall enforce name uniqueness within the X.500 name space to which they have been authorized.

The BPMA shall be responsible for ensuring name uniqueness in Certificates issued by the BBCA.

In the case where one Entity CA certifies another CA within that Entity, the certifying Entity CA shall impose restrictions on the name space authorized in the subordinate Entity CA, which are at least as restrictive as its own name constraints.

All Certificates issued by the BBKA shall have name constraints asserted that limit the name space of the subject CAs to name spaces that are appropriate for the subject CA domain.

**Practice Note:**

Entities should consider the following when including information concerning name uniqueness in their CPS:

1. What name forms shall be used; and
2. How they will allocate names within the Subscriber community to guarantee name uniqueness among current and past Subscribers (e.g., if "Joe Smith" leaves a CA's community of Subscribers, and a new, different "Joe Smith" enters the community of Subscribers, how will these two people be provided unique names?).

**3.1.6 Recognition, Authentication and Role of Trademarks**

No Stipulation

**3.1.7 Name Claim Dispute Resolution Procedure**

The BPMA shall resolve any name claims or collisions that are brought to its attention, in a manner that ensures interoperability.

Entity PMAs offering services to any organisation outside of itself shall have a dispute resolution procedure to ensure prompt resolution of any claims of this type.

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

## **3.2.2 Authentication of Organization Identity**

### **3.2.2.1 For Cross-Certificates**

Prior to issuance of any Cross-Certificates (as defined by section 10.1 and 10.2), a CA shall ensure the existence of the Organization stated in the "O" X.501 Distinguished name of the Subject. This shall include a verification of suitable proofs of address, registration of the Organization with an appropriate government agency, and its commercial status. The PMA of the issuing CA shall verify this information, as well as the authenticity of the requesting representative and the representative's authorization to act in the name of the organization.

### **3.2.2.2 Organization Affiliation**

For Subscriber Certificates that include the name of an Organization with whom a Subscriber is affiliated (eg: is an employee of, or is sponsored by), requests shall include the organization name, address, and documentation of the existence of the organization. The RA shall verify the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the organization.

## **3.2.3 Authentication of Individual Identity**

### **3.2.3.1 Common to all assurance Levels**

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

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

The process documentation and authentication requirements shall include the following:

- The identity of the person performing the identity verification; and
- A signed declaration by that person that he or she verified the identity of the applicant as required by this CP which may be met by establishing how the applicant is known to the verifier as required by this CP.

### **3.2.3.2 Basic Assurance Level**

For Certificates issued at the basic assurance level, the following information must be recorded:

- The full name, including surname and given name(s) of the applicant, and maiden name, if applicable; and
- The full name and legal status of the applicant's Employer; and
- An email address for the applicant; and
- A declaration signed by the applicant indicating his acceptance of the privacy policy outlined in section 9.4; and
- The date and time of the verification.

### **3.2.3.3 Medium Assurance Level**

For Certificates issued at the medium assurance level (Hardware and Software), the following information must be recorded:

- The full name, including surname and given name(s) of the applicant, and maiden name, if applicable; and
- The date and place of birth or other attribute(s) which may be used to uniquely identify the applicant; and
- The full name and legal status of the applicant's Employer; and
- A physical address or other suitable method of contact for the applicant; and
- A declaration signed by the applicant indicating his acceptance of the privacy policy outlined in section 9.4; and
- The date and time of the verification.

In addition to the above, the applicant shall:

- Present one (1) National Government-issued photo ID or two non-National Government IDs, one of which shall be a recent photo ID (e.g., Drivers License); and
- Have recorded unique identifying numbers from the Identifier (ID) of the verifier and from an ID of the applicant; and
- Sign a declaration of identity using a handwritten signature. This shall be performed in the presence of the person performing the identity authentication.

Identity shall be established by in-person proofing before the RA or Trusted Agent; information provided shall be verified to ensure legitimacy. A trust relationship between the Trusted Agent and the applicant, which is based on an in-person antecedent, may suffice as meeting the in-person identity-proofing requirement. Identity shall be established no more than thirty (30) days prior to the CA's signature on the subject Certificate.

## **3.2.4 Authentication of Component Identity**

### **3.2.4.1 Common to all Assurance Levels**

Some computing and communications components (routers, firewalls, servers, etc.) will be named as Certificate subjects. In such cases, the component (usually referred to as a "device") shall have a human sponsor (the "PKI Sponsor").

#### **3.2.4.2 Basic Assurance Level**

The PKI Sponsor shall be responsible for providing the following registration information:

- Equipment identification (e.g., serial number), MAC address, or service name (e.g., DNS name) sufficient to unique identify the Subject; and
- Equipment Public Keys; and
- Equipment authorisations and attributes (if any are to be included in the Certificate); and
- Contact information to enable the CA or RA to communicate with the sponsor when required.

The registration information shall be verified to an Assurance Level commensurate with the Certificate Assurance Level being requested.

Acceptable methods for performing this authentication and integrity checking include, but are not limited to:

- Verification of digitally signed messages sent from the PKI Sponsor (using Certificates of equivalent or greater assurance than that being requested); or
- In person registration by the sponsor, with the identity of the sponsor confirmed in accordance with the requirements of section 3.2.3.1 or 3.2.3.2.

#### **3.2.4.3 Medium Assurance Level**

The PKI Sponsor shall be responsible for providing the following registration information:

- Equipment identification (e.g., serial number), MAC address, or service name (e.g., DNS name) sufficient to unique identify the Subject; and
- Equipment Public Keys, if the private key is generated by the Subscriber; and
- Equipment authorisations and attributes (if any are to be included in the Certificate); and
- Contact information to enable the CA or RA to communicate with the sponsor when required.

The registration information shall be verified to an Assurance Level commensurate with the Certificate Assurance Level being requested.

Acceptable methods for performing this authentication and integrity checking include, but are not limited to:

- Verification of digitally signed messages sent from the PKI Sponsor (using Certificates of equivalent or greater assurance than that being requested); or
- In person registration by the sponsor, with the identity of the sponsor confirmed in accordance with the requirements of section 3.2.3.1 or 3.2.3.2.

### **3.2.5 Non-verified Subscriber Information**

Information that has not been verified shall not be included in Certificates.

#### **Practice Note:**

This includes: Information concerning affiliation included in the Subject Distinguished Name, as well as email addresses or other identifiers included in the Subject Alternative Names.

### **3.2.6 Validation of Authority**

#### **3.2.6.1 Authority to request Cross-Certification**

The PKI issuing a Cross-Certificate to another CA (the Subject CA) shall validate the requestor's authorization to act on behalf of the Subject CA. In addition to this, the Boost Operational Authority shall obtain the BPMAs approval prior to issuing any CA Certificates. For the BBCP, a Cross-Certificate to a PCA shall only be issued based on a successful mapping of the Subject CA's CP with this CP.

Any Certificates issued by any CA that contain explicit or implicit organisational affiliation shall be issued only pursuant to the stipulations of section 3.2.2.2

#### **3.2.7 Criteria for Interoperation**

A PCA or a Bridge CA shall adhere to the following requirements:

- Have a CP mapped to, and determined by the BPMA to be in conformance with this CP; and
- Operate a PKI that has undergone a successful compliance audit pursuant to Section 8.X.2 of this CP and as set forth in the Subject CA CP; and
- 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**

The CAs and subscribers shall be authenticated through use of their current, valid public key Certificates or by using the initial identity-proofing process as described above. For end entities with medium-software, medium-hardware or basic assurance Certificates, initial identity-proofing process needs to be carried once every nine years.

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

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

#### **3.3.2 Identification and Authentication for Re-key after Revocation**

No additional stipulations beyond those in 3.3.1

### **3.4. Identification and Authentication for Revocation Requests**

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.

If the Private Key is not available, alternate authentication methods may be available. Specific methods shall be described in the appropriate CPS.

#### **Practice note:**

Revocation authentication may be performed by sending a one-time code back to the email address listed in the Certificate and/or using pre-established questions and answers, or equivalent methods.

## **4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS**

### **4.1 Certificate Application**

This paragraph applies to entities seeking CA Certificates for their Principal CAs from the BBCA. The BPMA shall establish procedures for entities to use in applying for a Certificate from the BBCA and then publish those procedures. These processes shall minimally contain the following requirements and describe the following process:

Requests by a CA for CA Certificate from the BBCA shall be submitted to the BPMA using a procedure and application form developed by the BPMA. The BPMA shall make the procedures and application form available to all entities. The application shall be accompanied by a CP written to the format of [RFC3647]. Additionally, the application shall propose a mapping between the levels of assurance expressed in the Entity's CP, and those in this CP.

The BPMA shall evaluate the application in accordance with procedures that it shall develop and publish, and make a determination regarding whether or not to issue the requested Certificate(s), and what policy mappings to express in the Certificate(s). Boost Aerospace, based on BPMA Chair recommendation, and the applicant CA shall then enter into a MOA setting forth their respective responsibilities. The BPMA shall direct the Operational Authority to issue the Certificate(s). Upon issuance, each Certificate issued by a BBCA 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.

The BBCA may issue end-entity Certificates to trusted personnel where necessary for the internal operations of the BBCA. The BBCA shall not issue end-entity Certificates for any other reasons.

#### **4.1.1 Submission of Certificate Application**

For Certificate applications to the BBCA, an authorized representative of the Subject CA shall submit the application to the BPMA using the procedure and form developed for this purpose by the BPMA.

For submission of Certificate applications to an Entity CA, the Entity CA CP shall describe the submission process for its CAs and Subscribers.

#### **4.1.2 Enrollment Process and Responsibilities**

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

For Entity CAs as Issuers, the applicable CP shall describe the enrollment process for its Subject CAs and Subscribers.

## **4.2 Certificate Application Processing**

It is the responsibility of the CA and RA to verify that the information in Certificate applications is accurate. Applicable CP shall specify procedures to verify information in Certificate applications.

### **4.2.1 Performing Identification and Authentication Functions**

For the BBCA, the Operational Authority shall perform the identity-proofing of applicant Entity PCAs and other Subscribers.

For Entity CAs, the identity-proofing of subordinate CAs and Subscribers shall meet the requirements specified in the respective CP. To allow cross-certification, those requirements shall also meet the provision of this CP for Subscriber identity-proofing and authentication as specified in this CP. The applicable CP shall identify the components of the Entity PKI that are responsible for proofing or authenticating the Subscriber's identity in each case.

Prior to Certificate issuance, a Subscriber shall be required to sign a document containing the requirements the Subscriber shall protect the private key and use the Certificate and private key for authorized purposes only.

#### **Practice note:**

Once a Subscriber has undergone the identity-proofing process, it may be considered still valid for subsequent enrollments. For example, a user that has obtained an authentication Certificate may use this certificate to obtain an encryption Certificate at a later time if the initial certificate is still valid. This may be handled as a special case of Certificate modification.

### **4.2.2 Approval or Rejection of Certificate Applications**

For the BBCA, the BPMA may approve or reject a Certificate application.

The Entity CP shall identify the person or an organizational body that may accept or reject a Certificate application.

### **4.2.3 Time to Process Certificate Applications**

The Certificate application processing from the time the request/application is posted on the CA or RA system to Certificate issuance shall take no more than 30 days.

## **4.3 Certificate Issuance**

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

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

While the Subscriber may do most of the data entry, it is still the responsibility of the CA and the RA to verify that the information is correct and accurate. This may be accomplished through a system approach linking trusted databases containing personnel information, other equivalent authenticated mechanisms, or through personal contact with the Subscriber's sponsoring organization.

If databases are used to confirm Subscriber information, then these databases must be protected from unauthorized modification to a level commensurate with the level of assurance of the Certificate being sought. Specifically, the databases shall be protected using physical security controls, personnel security controls, cryptographic security controls, computer security controls, and network security controls specified for the RA elsewhere in this CP

#### **4.3.1 CA Actions during Certificate Issuance**

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

#### **4.3.2 Notification to Subscriber of Certificate Issuance**

A CA shall notify a subject (CA or End Entity Subscriber) of Certificate issuance.

### **4.4 Certificate Acceptance**

The MOA between Boost Aerospace and an Entity shall set forth responsibilities of all parties before the BPMA authorizes issuance of a CA Certificate by the BBCCA. Once a CA Certificate has been issued, its acceptance by the Entity shall commence interoperability with the BBCCA and thus triggers the Subject CA's obligations under the MOA and hence this CP.

#### **4.4.1 Conduct Constituting Certificate Acceptance**

For Certificates issued by the BBCCA, Certificate acceptance shall be governed by the MOA.

For Certificates issued by an Entity CA, Certificate acceptance shall be governed as set forth in the Entity CP.

#### **4.4.2 Publication of the Certificate by the CA**

Certificates shall be published in accordance with the stipulations of section 2.

#### **4.4.3 Notification of Certificate Issuance by the CA to Other Entities**

The Boost OA shall inform the BPMA of any Certificate issuance to a CA by the BBCCA.

When a PCA issues a Certificate to the BBCCA, the PCA shall notify the BPMA and Boost Operational Authority of the successful Certificate issuance.

Notification of Certificate issuance by the BBCA shall be provided to all cross-certified entities.

For Entity CAs, the BPMA shall be notified upon issuance of new CA Certificates.

## **4.5 Key Pair and Certificate Usage**

### **4.5.1 Subscriber Private Key and Certificate Usage**

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

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

### **4.5.2 Relying Party Public Key and Certificate Usage**

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

## **4.6 Certificate Renewal**

Renewing a Certificate means creating a new Certificate with the same name, key, and other information as the old one, but a new, extended validity period and a new serial number.

### **4.6.1 Circumstance for Certificate Renewal**

Certificates may be renewed in order to reduce the size of CRLs. A Certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the Subscriber name and attributes are unchanged. In addition, the validity period of the Certificate must not exceed the remaining lifetime of the private key, as specified in section 5.6. The time between identity proofing requirements specified in section 3.3.1 must also be respected; that is, the validity period of the new Certificate cannot exceed the time left before the next identity proofing is required. Once the Certificate is renewed, the original must be revoked as soon as possible.<sup>1</sup>

### **4.6.2 Who may Request Renewal**

A Subject may request the renewal of its Certificate.

A PKI Sponsor may request renewal of a component Certificate.

A CA may request renewal of its Subscriber Certificates, e.g., when the CA re-keys.

---

<sup>1</sup> In any case, the revocation must not occur later than one day after the renewed Certificate is issued.

### **4.6.3 Processing Certificate Renewal Requests**

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

- Initial registration process as described in section 4.1; or
- Identification & Authentication for Re-key as described in section 3.3, except the old key can also be used as the new key.

For CA Certificates issued by the BBCA, Certificate renewal also requires that a valid MOA exists between Boost and the Entity to whom the PCA belongs, and the term of the MOA is beyond the expiry period for the new Certificate.

### **4.6.4 Notification of New Certificate Issuance to Subscriber**

See section 4.3.2

### **4.6.5 Conduct Constituting Acceptance of a Renewal Certificate**

See section 4.4.1

### **4.6.6 Publication of the Renewal Certificate by the CA**

See section 4.4.2

### **4.6.7 Notification of Certificate Issuance by the CA to Other Entities**

See section 4.4.3

## **4.7 Certificate Re-Key**

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

### **4.7.1 Circumstance for Certificate Re-key**

A CA may issue a new Certificate to the Subject when the Subject has generated a new key pair and is entitled to a Certificate. The CA must only re-key when the old private key of the same type corresponding to the public key in a Certificate issued to a Subscriber has reached the end of the lifetime period described in section X.X.X

### **4.7.2 Who may Request Certification of a New Public Key**

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

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

### **4.7.3 Processing Certificate Re-keying Requests**

The stipulations of section 4.6.3 shall apply.

#### **4.7.4 Notification of New Certificate Issuance to Subscriber**

See section 4.3.2.

#### **4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate**

See section 4.4.1

#### **4.7.6 Publication of the Re-keyed Certificate by the CA**

See section 4.4.2

#### **4.7.7 Notification of Certificate Issuance by the CA to Other Entities**

See section 4.4.3

### **4.8 Certificate Modification**

Updating a Certificate means creating a new Certificate that has the same or a different key and a different serial number, and that it differs in one or more other fields, from the old Certificate. For example, an Entity CA may choose to update a Certificate of a Subscriber 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 further re-keyed, renewed, or updated.

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 the trusted agent in order for an updated Certificate having the new name to be issued.

#### **4.8.1 Circumstance for Certificate Modification**

A CA may issue a new Certificate to a Subject when some of the Subject information changes (e.g.: name change due to change in marital status), or when requirements necessitate the modification of information included in the Certificate (new extended key usage needed to support smart card login).

#### **4.8.2 Who may Request Certificate Modification**

A Subject may request modification of its Certificate.

A PKI Sponsor may request may request modification of component Certificate.

#### **4.8.3 Processing Certificate Modification Requests**

The stipulations of section 4.6.3 shall apply.

#### **4.8.4 Notification of New Certificate Issuance to Subscriber**

See section 4.3.2

#### **4.8.5 Conduct Constituting Acceptance of Modified Certificate**

See section 4.4.1

#### **4.8.6 Publication of the Modified Certificate by the CA**

See section 4.4.2

## **4.8.7 Notification of Certificate Issuance by the CA to Other Entities**

See section 4.4.3

## **4.9 Certificate Revocation and Suspension**

### **4.9.1 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 or affiliation components of any names in the Certificate become invalid; or
- An organization terminates its relationship with the CA such that it no longer provides affiliation information; or
- Privilege attributes asserted in the Subject's Certificate are reduced; or
- The Subject can be shown to have violated the stipulations of its agreement; or
- The private key is suspected of compromise; or
- The Subject or other authorized party (as defined in the applicable CP or CPS) asks for his/her Certificate to be revoked.

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

Entity PKI shall request that BBCA revoke their Cross-Certificate if they do not meet the stipulations of the Certificate policies listed in their Certificate, including the Boost Aerospace policy OIDs.

### **4.9.2 Who Can Request Revocation of a Certificate**

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

In the case of Certificates issued by the BBCA, the BPMA may request revocation of a Certificate.

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

### **4.9.3 Procedure for Revocation Request**

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. If the Private Key is not available anymore, specific identification measures may be used, as described in section 3.4.

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 the BBCCA 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 BPMA 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 the BBCCA, the Operational Authority shall seek guidance from the BPMA before revocation of the Certificate except when the BPMA is not available and there is an emergency situation such as:

- Request from the Subject CA for reason of key compromise; or
- 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, CPS, or MOA to a degree that threatens the integrity of the Boost Aerospace PKI.

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

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

#### **4.9.4 Revocation Request Grace Period**

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

#### **4.9.5 Time within which CA must Process the Revocation Request**

The BBCCA shall process all revocation requests within 12 hour of receipt of such a request.

For Entity CAs, revocation request processing time shall be as follows:

For Basic Assurance level Certificates – Within 24 hours of receipt of request.

For Medium Assurance level Certificates – Within 18 hours of receipt of request.

#### 4.9.6 Revocation Checking Requirements for Relying Parties

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

#### 4.9.7 CRL Issuance Frequency

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

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

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

The following table outlines the CRL issuance frequency requirements for all assurance levels:

	<b>CRL Issuance Frequency</b>
<b>Routine</b>	At least once every 30 days for Off-line Roots and Off-line Bridge CAs; At Least Once every 24 hours for all others
<b>Loss or Compromise of Private Key</b>	Within 18 Hours of Notification
<b>CA Compromise</b>	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 Boost Operational Authority upon Emergency CRL issuance. This requirement shall be included in the MOA between the Boost Aerospace and the Entity.

#### 4.9.8 Maximum Latency for CRLs

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

#### **4.9.9 Online Revocation Checking Availability**

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

If on-line revocation/status checking is supported by a CA, the latency of Certificate status information distributed on-line by the CA or its delegated status responders shall meet or exceed the requirements for CRL issuance stated in 4.9.7. Furthermore, such CAs shall support the CA-Delegated trust model as outlined in [RFC2560].

#### **4.9.10 Online Revocation Checking Requirements**

The CAs are not required to operate an OCSP Responder covering the Certificates they issue. The BBKA PKI Repository shall contain and publish a list of all OCSP Responders operated by the BBKA and by the PKIs cross-certified with the BBKA.

#### **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. However, even if such alternates are made available by a CA, they shall at least support publication of CRL information as specified in sections 2 and 4.9.7.

#### **4.9.12 Special Requirements Related To Key Compromise**

No additional stipulations beyond section 4.9.7

#### **4.9.13 Circumstances for Suspension**

CAs operating under this CP shall not support Suspension of Certificates.

#### **4.9.14 Who can Request Suspension**

N/A

#### **4.9.15 Procedure for Suspension Request**

N/A

#### **4.9.16 Limits on Suspension Period**

N/A

### **4.10 Certificate Status Services**

CAs operating under this CP are not required to support Certificate status services such as SCVP [RFC5055].

#### **4.10.1 Operational Characteristics**

No Stipulation

#### **4.10.2 Service Availability**

Relying parties are bound to their obligations covered by this CP irrespective of the availability of the Certificate Status service.

#### **4.10.3 Optional Features**

No Stipulation

#### **4.11 End Of Subscription**

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

#### **4.12 Key Escrow and Recovery**

##### **4.12.1 Key Escrow and Recovery Policy and Practices**

Under no circumstances shall a CA key or end entity signature or identity key be escrowed by a third-party.

This CP requires the Entity PKI to escrow decryption private keys (see Section 6.2.3). Entity PKI shall develop a Key Recovery Practices Statement (KRPS) that complies with the Boost Key Recovery Policy (KRP).

##### **4.12.2 Session Key Encapsulation and Recovery Policy and Practices**

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

# 5 FACILITY MANAGEMENT & OPERATIONAL CONTROLS

## 5.1 Physical Controls

### 5.1.1 Site Location & Construction

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

### 5.1.2 Physical Access

#### 5.1.2.1 CA Physical Access

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

- Ensure no unauthorized access to the hardware is permitted; and
- Ensure all removable media and paper containing sensitive plain-text information is stored in secure containers; and
- Be manually or electronically monitored for unauthorized intrusion at all times; and
- Ensure an access log is maintained and inspected periodically; and
- Provide at least three layers of increasing security such as perimeter, building, and CA room; and
- Require two person physical access control to both the cryptographic module and computer system; and
- Removable cryptographic modules shall be deactivated prior to storage. When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules shall be placed in secure containers.

Activation data shall either be 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.

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

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when "open", and secured when "closed"); and

- For off-line systems, all equipment other than the PKI Repository is shut down); and
- Any security containers are properly secured; and
- Physical security systems (e.g., door locks, vent covers) are functioning properly; and
- The area is secured against unauthorized access.

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

#### **5.1.2.2 RA Equipment Physical Access**

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

#### **5.1.3 Power and Air Conditioning**

CAs shall have backup power sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. PKI Repositories shall be provided with 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**

No stipulation

#### **5.1.5 Fire Prevention & Protection**

No stipulation

#### **5.1.6 Media Storage**

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

#### **5.1.7 Waste Disposal**

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

### 5.1.8 Off-Site backup

Full system backups of CAs, sufficient to recover from system failure, shall be made as described in the respective CPS. For online CAs, this must be performed on a periodic schedule not less than once every 7 days; for offline CAs, this must be performed at the end of every session where the CA is booted. At least one full backup copy shall be stored at an off-site 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 to that of the operational CA.

Accessibility of the off-site copy and restore procedures must take into account the maximum delays for the publication of revocation information, as described in section 4.9.7.

## 5.2 Procedural Controls

### 5.2.1 Trusted Roles

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

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

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

The following sections define these and other trusted roles.

#### 5.2.1.1 Administrator

The administrator shall be responsible for:

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

Administrators shall not issue Certificates to Subscribers.

#### **5.2.1.2 Officer**

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

- Registering new subscribers and requesting the issuance of Certificates; and
- Verifying the identity of subscribers and accuracy of information included in Certificates; and
- 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; and
- Performing or overseeing internal compliance audits to ensure that the CA is operating in accordance with its CPS.

#### **5.2.1.4 Operator**

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

#### **5.2.1.5 Registration Authority**

An RA's responsibilities are:

- Verifying identity, pursuant to section 3.2; and
- Entering Subscriber information, and verifying correctness; and
- Securely communicating requests to and responses from the CA; and
- Receiving and distributing Subscriber Certificates.

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

#### **5.2.1.6 CSA Roles**

A CSA shall have, at minimum the following roles:

The *CSA administrator* shall be responsible for:

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

The *CSA Audit Administrator* shall be responsible for:

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

The *CSA Operator* shall be responsible for:

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

#### **5.2.1.7 CMS Roles**

A CMS shall have at least the following roles.

The *CMS administrator* shall be responsible for:

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

The *CMS Audit Administrator* shall be responsible for:

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

The *CMS Operator* shall be responsible for:

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

#### **5.2.1.8 PKI Sponsor**

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

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

#### **5.2.1.9 Trusted Agent**

A Trusted Agent is responsible for:

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

A Trusted Agent need **not** be a Trusted role, but should have been issued a credential that is equal to or higher assurance level than the credentials for which they are proofing the identities.

#### **5.2.2 Number of Persons Required per Task**

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

- CA Signing key generation; or

- CA Signing key activation; or
- CA Signing 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 Auditor Administrator Role.

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

### **5.2.3 Identification and Authentication for Each Role**

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

All Trusted Roles who operate a CMS shall be allowed access only when authenticated using a method commensurate with medium-hardware assurance level.

### **5.2.4 Roles Requiring Separation of Duties**

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

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

Individuals who assume an Officer role may not assume an Administrator or Audit Administrator role;

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

No individual shall be assigned more than one identity.

## **5.3 Personnel Controls**

### **5.3.1 Qualifications, Experience, and Clearance Requirements**

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

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

- Have successfully completed an appropriate training program; and
- Have demonstrated the ability to perform their duties; and

- Be trustworthy; and
- Have no other duties that would interfere or conflict with their duties for the trusted role; and
- Have not been previously relieved of duties for reasons of negligence or non-performance of duties; and
- Have not been denied a security clearance, or had a security clearance revoked for cause<sup>2</sup>; and
- Have not been convicted of a serious criminal offense; and
- Be appointed in writing by an approving authority.

For PKIs operated at medium-software, and/or medium-hardware, each person filling a trusted role shall satisfy at least one of the following requirements:

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

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

### **5.3.2 Background Check Procedures**

All persons filling CA trusted roles, CSA trusted roles, Trusted Agent, and RA roles shall have completed a background investigation as allowed by applicable national law or regulation. The scope of the background check shall include the following areas covering the past five (5) years and should be refreshed every five (5) years:

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

---

<sup>2</sup> Practice Note: In order to make the determination if a person was denied clearance or had clearance revoked for cause, it is sufficient to rely on the local Facility Security Officer (FSO) database, and assertions by the person on security clearance forms.

Adjudication of the background investigation shall be performed in accordance with the requirements of the appropriate national adjudication authority.

The results of these checks shall not be released except as required in sections X.X.X and X.X.X.

Background check procedures shall be described in the CPS.

### **5.3.3 Training Requirements**

All personnel performing duties with respect to the operation of a CA, CSA, CMS or a RA shall receive comprehensive training.

Training shall be conducted in the following areas:

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

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

### **5.3.4 Retraining Frequency and Requirements**

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

### **5.3.5 Job Rotation Frequency and Sequence**

No Stipulation.

### **5.3.6 Sanctions for Unauthorized Actions**

The responsible PMA shall ensure appropriate administrative and disciplinary actions are taken against personnel who violate this policy.

### **5.3.7 Independent Contractor Requirements**

Sub-Contractor personnel employed to perform functions pertaining to CA, CSA, CMS or RA operations shall meet applicable requirements set forth in this CP (e.g., all requirements of section 5.3).

### **5.3.8 Documentation Supplied To Personnel**

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

## 5.4 Audit Logging Procedures

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

### 5.4.1 Types of Events Recorded

All security auditing capabilities of the CA, CMS, CSA, and RA operating system and the CA, CMS, CSA, and RA applications required by this CP shall be enabled. As a result, most of the events identified in the 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; and
- The date and time the event occurred; and
- Success or failure where appropriate; and
- The identity of the entity and/or operator that caused the event; and
- A message from any source requesting an action by a CA is an auditable event.

The message must include message date and time, source, destination and contents.

The following events shall be audited:

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

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

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

<b>Auditable Event</b>	<b>CA</b>	<b>CSA</b>	<b>RA</b>	<b>CMS</b>
Known or suspected violations of physical security	X	X	X	X
<b>ANOMALIES</b>				
Software error conditions	X	X	X	X
Software check integrity failures	X	X	X	X
Receipt of improper messages	X	X	X	X
Misrouted messages	X	X	X	X
Network attacks (suspected or confirmed)	X	X	X	X
Equipment failure	X	-	-	X
Electrical power outages	X	-	-	X
Uninterruptible Power Supply (UPS) failure	X	-	-	X
Obvious and significant network service or access failures	X	-	-	X
Violations of Certificate Policy	X	X	X	X
Violations of Certification Practice Statement	X	X	X	X
Resetting Operating System clock	X	X	X	X

#### **5.4.2 Frequency of Processing Audit Logs**

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

#### **5.4.3 Retention Period for Audit Logs**

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

#### **5.4.4 Protection of Audit Logs**

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

- Only authorized people<sup>3</sup> have read access to the logs; and
- Only authorized people may archive audit logs; and
- Audit logs are not modified.

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

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

#### 5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries shall be backed up at least once every 30 days. A copy of the audit log shall be sent off-site every 30 days in accordance with a process to be described in the CPS.

#### 5.4.6 Audit Collection System (internal vs. external)

The audit log collection system may or may not be external to the CA, CMS, CSA, or RA. Audit processes shall be invoked at system startup, and cease only at system shutdown. Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the CA shall determine whether to suspend CA operation until the problem is remedied.

#### 5.4.7 Notification to Event-Causing Subject

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

#### 5.4.8 Vulnerability Assessments

No stipulation beyond section 5.4.2

### 5.5 Records Archival

#### 5.5.1 Types of Records Archived

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

Data To Be Archived	CA	CSA	RA	CMS
Certification Practice Statement	X	X	X	X
Contractual obligations	X	X	X	X

<sup>3</sup> For the CA, CMS, and CSA, the authorized individual shall be the Audit Administrator. For RA, the authorized individual shall be a system administrator other than the RA.

<b>Data To Be Archived</b>	<b>CA</b>	<b>CSA</b>	<b>RA</b>	<b>CMS</b>
System and equipment configuration	X	X	-	X
Modifications and updates to system or configuration	X	X	-	X
Certificate requests	X	-	-	X
Revocation requests	X	-	-	X
Subscriber identity authentication data as per Section 3.2	X	N/A	X	X
Documentation of receipt and acceptance of Certificates	X	N/A	X	X
Documentation of receipt of Tokens	X	N/A	X	X
All Certificates issued or published	X	N/A	N/A	X
Record of Component CA Re-key	X	X	X	X
All CRLs and CRLs issued and/or published	X	N/A	N/A	N/A
All Audit Logs	X	X	X	X
Other data or applications to verify archive contents	X	X	X	X
Documentation required by compliance auditors	X	X	X	X

### **5.5.2 Retention Period for Archive**

The retention period for archive data shall depend on the legal and business requirements and is set forth in the respective CPS. However, the archive data must be kept for a minimum retention period of ten (10) years and six (6) months.

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

Applications required processing the archive data shall also be maintained for the minimum retention period specified above.

### **5.5.3 Protection of Archive**

No unauthorized user shall be permitted to write to, modify, or delete the archive. For the CA, CMS, and CSA, the authorized individuals are Audit Administrators. For the RA, authorized individuals are someone other than the RA (e.g., Information Assurance Officer or IAO). The contents of the archive shall not be released except as determined by the BPMA for the BBKA, Entity PMA for the Entity CA, or as required by law. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. Archive media shall be stored in a safe, secure storage facility separate from the component (CA, CMS, CSA, or RA) with physical and procedural security controls equivalent or better than those for component.

### **5.5.4 Archive Backup Procedures**

The CPS or a referenced document shall describe how archive records are backed up, and how the archive backups are managed.

### 5.5.5 Requirements for Time-Stamping of Records

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

### 5.5.6 Archive Collection System (internal or external)

No Stipulation

### 5.5.7 Procedures to Obtain & Verify Archive Information

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

## 5.6 Key Changeover

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

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

Key	1024 Bit Keys		2048 Bit Keys		4096 Bit Keys	
	Private Key	Certificate	Private Key	Certificate	Private Key	Certificate
BBCA	N/A	N/A	5 years	10 years	5 years	10 years
PCA	N/A	N/A	20 years	10 years	20 years	10 years
Root CA	N/A	N/A	20 years	20 years	25 years	25 years
Intermediate CA (offline)	N/A	N/A	20 years	20 years	25 years	25 years
Intermediate CA (online)	N/A	N/A	10 years	20 years	10 years	20 years
Signing CA	N/A	N/A	5 years	10 years	5 years	10 years
Bridge CA	N/A	N/A	5 years	10 years	5 years	10 years
Subscriber Identity or Signature	N/A	N/A	3 years	3 years	3 years	3 years
Subscriber Encryption	N/A	N/A	3 years	3 years	3 years	3 years
Code Signer	3 years	3 years	10 years	10 years	10 years	10 years
OCSF Responder	N/A	N/A	3 years	1 month	3 years	1 month
SCVP Server	N/A	N/A	3 years	3 years	3 years	3 years
Server	3 years	3 years	3 years	3 years	3 years	3 years

Timestamp Server	N/A	N/A	10 years	20 years	10 years	20 years
------------------	-----	-----	----------	----------	----------	----------

## 5.7 Compromise and Disaster Recovery

### 5.7.1 Incident and Compromise Handling Procedures

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

The BPMA and the PMAs of cross-certified Entity PKIs shall be notified if any of the following cases occur:

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

The BPMA and the PMAs of cross-certified Entity PKIs shall be notified if any of the following cases occur:

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

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

A CA Operational Authority shall reestablish operational capabilities as quickly as possible in accordance with procedures set forth in the respective CPS.

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

### 5.7.2 Computing Resources, Software, and/or Data are Corrupted

If a 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.

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<sup>4</sup> notified immediately.

This will allow other CAs to protect their Subscribers' interests as Relying Parties. The CA shall reestablish revocation capabilities as quickly as possible in accordance with procedures set forth in the respective CPS. If revocation capability cannot be established in a reasonable time-frame, the CA shall determine whether to request revocation of its Certificate(s). If the CA is a Root CA, the CA shall determine whether to notify all subscribers that use the CA as a trust anchor to delete the trust anchor.

### **5.7.3 Private Key Compromise Procedures**

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

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

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

If a CSA key is compromised, all Certificates issued to the CSA shall be revoked, if applicable. The CSA will generate a new key pair and request new Certificate(s), if applicable. 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 a RA signature keys are compromised, lost, or suspected to be compromised:

- The RA Certificate shall be immediately revoked; and
- A new RA key pair shall be generated in accordance with procedures set forth in the applicable CPS; and

---

<sup>4</sup> With confidentiality, source authentication, and integrity security services applied.

- New RA Certificate shall be requested in accordance with the initial registration process set elsewhere in this CP; and
- All Certificate registration requests approved by the RA since the date of the suspected compromise shall be reviewed to determine which one are legitimate; and
- For those Certificates requests or approval than can not be ascertained as legitimate, the resultant Certificates shall be revoked and their subjects (i.e., subscribers) shall be notified of revocation.

#### **5.7.4 Business Continuity Capabilities after a Disaster**

In the case of a disaster whereby a CA installation is physically damaged and all copies of the CA Signing Key are destroyed as a result, the CA shall request that its Certificates be revoked. The CA shall follow the steps outlined in section 5.7.3 above.

#### **5.8 CA, CSA, and RA Termination**

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

In the event of a CA termination, the Entity responsible shall provide notice to all cross certified CAs prior to the termination. Additionally, in the case of BBKA termination, Entities will be given as much advance notice as circumstances permit, and attempts to provide alternative sources of interoperation will be sought.

A CA, CSA, and RA shall archive all audit logs and other records prior to termination.

A CA, CSA, and RA shall destroy all its private keys upon termination.

CA, CSA, and RA archive records shall be transferred an appropriate authority such as the PMA responsible for the entity.

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

## 6 TECHNICAL SECURITY CONTROLS

### 6.1 Key Pair Generation and Installation

#### 6.1.1 Key Pair Generation

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

Entity	FIPS 140-1/2 Level or Common Criteria EAL	Hardware or Software	Same Module
CA	3 / 4+	Hardware	Same
CMS	2 / 4+	Hardware	Same
RA	2 / 4+	Hardware	Same
OCSP Responder	2 / 4+	Hardware	Same
SCVP Server	2 / 4+	Hardware	Same
Code Signing	2 / 4+	Hardware	Same
Content Signing	2 / 4+	Hardware	Same
End Entity Signature or Identity (basic)	No Requirement	Software	No Requirement
End Entity Encryption (basic)	No Requirement	Software	No Requirement
End Entity Signature or Identity (medium-software)	1 / 4+	Software	No Requirement
End Entity Encryption (medium-software)	1 / 4+	Software	No Requirement
End Entity Signature or Identity (medium-hardware)	2 / 4+	Hardware	Same
End Entity Encryption (medium-hardware)	2 / 4+	Hardware	No Requirement
Server (basic)	No Requirement	Software	No Requirement
Server (medium-software)	1 / 4+	Software	No Requirement
Server (medium-hardware)	2 / 4+	Hardware	Same

When using Common Criteria-evaluated components, the associated security target must describe a target of evaluation which covers the hardware and software aspects of the required cryptographic functions.

Random numbers for medium-hardware assurance level keys shall be generated in FIPS 140-2 Level 2 or Common Criteria EAL 4+ validated hardware cryptographic modules.

When Private Keys are not generated on the token to be used, originally generated Private Keys shall be destroyed after they have been transferred to the token. This does not prohibit the key generating modules to further act 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 that the security requirements for procedures were followed. The documentation of the procedure shall be detailed enough to show that appropriate role separation was used. An independent third party shall validate the process.

### **6.1.2 Private Key Delivery to Subscriber**

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

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

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

- Anyone who generates a private signing key for a Subscriber shall not retain any copy of the key after delivery of the private key to the Subscriber; and
- The private key shall be protected from activation, compromise, or modification during the delivery process; and
- The Subscriber shall acknowledge receipt of the private key(s).

Delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers.

For hardware modules, accountability for the location and state of the module shall be maintained until the Subscriber accepts possession of it.

For electronic delivery of private keys, the key material shall be encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data shall be delivered using a separate secure channel.

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

### 6.1.3 Public Key Delivery to Certificate Issuer

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

### 6.1.4 CA Public Key Delivery to Relying Parties

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

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

### 6.1.5 Key Sizes

If the BPMA determines that the security of a particular algorithm may be compromised, it may require the CAs to revoke the affected Certificates. All Certificates and Transport Layer Security (TLS) protocols shall use the following algorithm suites.

<b>Cryptographic Function</b>	<b>Expire on or before 12/31/2010</b>	<b>Expire after 12/31/2010</b>
Signature	1024 bit RSA per FIPS 186-2 For ECDSA, per FIPS 186-2, 193 bit prime field or 163 bit binary field	2048 bit RSA per FIPS 186-2 For ECDSA, per FIPS 186-2, 224 bit prime field or 233 bit binary field
Hashing	SHA-1	SHA-1 for Certificates issued before 1/1/2014; SHA-256 for Certificates issued on or after 1/1/2014
Public Key Encryption	1024 bit RSA per PKCS 1 For ECDH, per SP 800-56A, 193 bit prime field or 163 bit binary field	2048 bit RSA per PKCS 1 For ECDH, per SP 800-56A, 224 bit prime field or 233 bit binary field
Symmetric	3 Key TDES or AES	3 Key TDES or AES

Cryptographic Function	Expire on or before 12/31/2010	Expire after 12/31/2010
Encryption		

Regardless, all CAs shall use 2048 bit RSA or stronger.

CSAs shall use the same signature algorithms, key sizes, and hash algorithms as used by the CA to sign the CRL.

As specified in section 10, Certificate field order and Certificate Serial Numbers must be assigned in an unpredictable manner to increase the difficulty of cryptographic attacks.

### **6.1.6 Public Key Parameters Generation and Quality Checking**

Medium assurance RSA keys shall be generated in accordance with ANSI X9.31.

ECDSA and ECDH keys shall be generated in accordance with FIPS 186-2. Curves from FIPS 186-2 shall be used.

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

The use of a specific key is determined by the keyUsage extension in the X.509 Certificate. The Certificate Profiles in section 10 specify the allowable values for this extension for different types of Certificates defined under this CP, and all CAs issuing Certificates in accordance with this CP must adhere to those values.

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

## **6.2 Private Key Protection and Cryptographic Module Engineering Controls**

### **6.2.1 Cryptographic Module Standards and Controls**

The relevant standard for cryptographic modules are [FIPS PUB 140-2] and [Common Criteria]. The BPMA may determine that other, comparable, validation, certification, or verification standards are sufficient. Such standards, once approved will be published by the BPMA. Cryptographic modules shall be validated to the FIPS 140-2 level or Common Criteria EAL identified in this section, or validated, certified, or verified to the aforementioned equivalent standards.

Additionally, the BPMA reserves the right to review technical documentation associated with any cryptographic modules under consideration for use by the CAs.

The table in section 6.1.1 summarizes the minimum requirements for cryptographic modules; higher levels may be used. In addition, medium-hardware tokens shall not output private keys in plaintext form.

### **6.2.2 Private Key Multi-Person Control**

Activation a CA or CMS private signing key shall require action by at least two persons as specified in section 5.X.X

### **6.2.3 Private Key Escrow**

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

The end entity private keys used solely for decryption shall be escrowed prior to the generation of the corresponding Certificates. Such escrow must be in accordance with the KRP specified in section 4.12.

### **6.2.4 Private Key Backup**

#### **6.2.4.1 Backup of CA Private Signature key**

The CA private signature keys shall be backed up under the same multi-person control as the operational signature key. A single backup copy of the signature key shall be stored at or near the CA location. A second backup copy shall be kept at the CA backup location. Procedures for CA private signature key backup shall be included in the appropriate CPS and shall meet the multiparty control requirement of Section 6.2.2.

#### **6.2.4.2 Backup of Subscriber Private Signature and Identity Keys**

Subscriber private keys whose corresponding public key is contained in a Signature or Identity Certificate asserting the basic or medium-software assurance levels may be backed up or copied, but must be held in the Subscriber's control.

Subscriber private keys whose corresponding public key is contained in a Signature or Identity Certificate asserting the medium-hardware may not be backed up or copied.

#### **6.2.4.3 CSA Private Key Backup**

If backed up, the CSA private signature keys shall be backed up under the same single or multi-person control as the signature key is invoked. A single backup copy of the signature key may be stored at or near the CSA location. A second backup copy may be kept at the CSA backup location. Procedures for CSA private signature key backup shall be included in the appropriate CPS.

#### **6.2.4.4 CMS Signing Key Backup**

The CMS private keys shall be backed up under the same multi-person control as the operational content signing key. A single backup copy of the signature key shall be stored at or near the content signing system location. A second backup copy shall be kept at a backup location.

### **6.2.5 Private Key Archival**

Private keys associated with a Certificate which was issued according to the Signature or Identity profiles shall not be archived by the CA.

Private keys used for decryption must be archived according to the requirements included in the KRP specified in section 4.12.

### **6.2.6 Private Key Transfer into or from a Cryptographic Module**

Private keys shall be generated by and remain in a cryptographic module as specified by the table in section 6.1.1.

### **6.2.7 Private Key Storage on Cryptographic Module**

The cryptographic module may store Private Keys in any form as long as the keys are not accessible without authentication mechanism that is in compliance with the FIPS 140-1/2 rating or Common Criteria Protection Profiles 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). Acceptable means of authentication include but are not limited to pass-phrases, PINs or biometrics. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

For basic assurance level, distinct activation beyond that which gives access to the application keystore is not required.

### **6.2.9 Methods of Deactivating Private Key**

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

### **6.2.10 Method of Destroying Private Key**

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

### **6.2.11 Cryptographic Module Rating**

See sections 6.1.1 and 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 table in section 5.6

## **6.4 Activation Data**

### **6.4.1 Activation Data Generation and Installation**

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

### **6.4.2 Activation Data Protection**

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

### **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, CMS, CSA and RA shall include the following functionality:

- Require authenticated logins; and
- Provide Discretionary Access Control, including managing privileges of users to limit users to their assigned roles; and
- Provide a security audit capability (See Section 5.4); and

- Prohibit object re-use; and
- Require use of cryptography for session communication and database security; and
- Require a trusted path for identification and authentication; and
- Provide domain isolation for processes; and
- Provide self-protection for the operating system; and
- Require self-test security related CA services (e.g., check the integrity of the audit logs); and
- Support recovery from key or system failure.

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

The computer system shall be configured with minimum of the required accounts, network services, and, for CAs operating at assurance levels other than basic level of assurance, no remote login.

### **6.5.2 Computer Security Rating**

No stipulations

## **6.6 Life-Cycle Technical Controls**

### **6.6.1 System Development Controls**

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

- Use software that has been designed and developed under a formal, documented development methodology; and
- Hardware and software procured shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase); and
- Hardware and software developed shall be developed in a controlled environment, and the development process shall be defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software; and
- 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; and
- The hardware and software shall be dedicated to performing the PKI activities. There shall be no other applications; hardware devices, network connections, or component software installed which are not part of the PKI operation; and

- Proper care shall be taken to prevent malicious software from being loaded onto the equipment.

Only applications required to perform the PKI operations shall be obtained from sources authorized by local policy. CA, CSA, and RA hardware and software shall be scanned for malicious code on first use and periodically thereafter.

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

### **6.6.2 Security Management Controls**

The configuration of the CA, CMS, and CSA system as well as any modifications and upgrades shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the CA, CMS, and CSA software or configuration. A formal configuration management methodology shall be used for installation and ongoing maintenance of the CA and CMS system. The CA and CSA software, when first loaded, shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use. For the BBKA, the integrity of the software shall be verified by the Boost Aerospace Operational Authority at least once every 7 days (e.g., in conjunction with CRL publication).

### **6.6.3 Life Cycle Security Controls**

No Stipulation.

## **6.7 Network Security Controls**

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

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

## **6.8 Time Stamping**

For timestamps on audit records, all CA and CSA components shall regularly synchronize with a time service such as **FIXME:REFERENCE** Atomic Clock or **FIXME:REFERENCE** Network Time Protocol (NTP) Service. Time derived from the time service shall be used for establishing the time of:

- Initial validity time of a Subscriber's Certificate; and
- Revocation of a Subscriber's Certificate; and
- Posting of CRL updates; and
- OCSP or other CSA responses.

Asserted times shall be accurate to within three minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events as listed in Section 5.4.

# 7 CERTIFICATE, CRL, AND OCSP PROFILES

## 7.1 Certificate Profile

### 7.1.1 Version Numbers

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

### 7.1.2 Certificate Extensions

Any CAs asserting critical private extensions shall be interoperable in their intended community of use.

Issuer CA and Subscriber Certificates may include any extensions as specified by RFC 3280 in a Certificate, but must include those extensions required by this CP. Any optional or additional extensions shall be non-critical and shall not conflict with the Certificate and CRL profiles defined in this CP. Section 10 contains these Certificate profiles.

### 7.1.3 Algorithm Object Identifiers

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

sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
ecdsa-with-Sha1	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) sha1(1)}
ecdsa-with-Sha256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) specified(3) sha256(2)}

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

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

### 7.1.4 Name Forms

The Subject and Issuer fields of the Certificate shall be populated with a unique Distinguished Name in accordance with one or more of the X.500 series standards, with the attribute type as further constrained by [RFC5280], and section 3.1.2.

Subject and Issuer fields shall include attributes as detailed in the table below.

## Issuer and Subject Name Form (CAs)

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

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

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

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

When issuing Certificates to another Bridge CA (say CA X), BBCA shall use the excluded subtree field to exclude all other Bridge CAs except X.

The Issuer CA may obscure a Subscriber Subject name to meet local privacy regulations as long as such name conforms to the requirements in section 3.1.3. Issuer names may not be obscured. Issuer CAs may assert critical or non-critical name constraints beyond those specified in the Certificate Profiles.

### 7.1.6 Certificate Policy Object Identifier

CA and Subscriber Certificates issued under this CP shall assert one or more of the basic, medium-software or medium-hardware Certificate policy OIDs listed in section 1.2 of this CP. This CP assumes a strict ordering among these policies, with medium-hardware being the highest assurance level. When a CA asserts a policy OID, shall also assert all lower assurance policy OIDs.

The following table should be used when populating the Certificate Policy fields for the different assurance levels:

Assurance level of Certificate	Policy OIDs asserted
Basic	id-basic
Medium-Software	id-basic id-medium-software
Medium-Hardware	id-basic id-medium-software id-medium-hardware

### 7.1.7 Usage of Policy Constraints Extension

The BBCA shall assert the policy constraints extension to inhibit policy mapping by the PCAs.

The Issuer PCAs are required to adhere to the Certificate profiles described in section 10 of this CP since inhibiting policy mapping may limit interoperability.

The BBCA will assert inhibit policy mapping with skipCerts value = 1 when issuing Certificates to other Bridge CAs. It is assumed that a certification path will entail no more than two Bridge CAs. In other words, all Bridge – Bridge interoperability shall be on a bilateral basis.

### **7.1.8 Policy Qualifiers Syntax and Semantics**

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

### **7.1.9 Processing Semantics for the Critical Certificate Policy Extension**

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

## **7.2 CRL Profile**

### **7.2.1 Version Numbers**

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

### **7.2.2 CRL and CRL Entry Extensions**

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

Section 10.14 contains the CRL formats.

## **7.3 OCSP Profile**

### **7.3.1 Version Number**

The version number for request and responses shall be v1.

### **7.3.2 OCSP Extensions**

OCSP requests and responses shall be in accordance with RFC 2560. Sections 10.13 and 10.14 contain the OCSP request and response formats. All OCSP Responses shall support the nonce extension.

## **8. Compliance Audit and Other Assessment**

CAs shall have a compliance audit mechanism in place to ensure that the requirements of their CP/CPS and the provisions of the MOA are being implemented and enforced.

### **8.1 Frequency or Circumstances of Assessments**

All CAs, CMSs, 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 the applicable CP. The compliance auditor must perform such compliance audits as a primary responsibility. The applicable CPS shall identify the compliance auditor and justify the compliance auditor's qualifications.

### **8.3 Assessor's Relationship to Assessed Entity**

The compliance auditor shall be a firm, which is independent from the entity being audited. The BPMA shall determine whether a compliance auditor meets this requirement.

### **8.4 Topics Covered by Assessment**

The purpose of a compliance audit shall be to verify that a component operates in accordance with the applicable CP, the component CPS, and the applicable MOAs between the Entity PKI, Boost Aerospace, and other Entities (e.g. CertiPath).

### **8.5 Actions Taken as a Result of Deficiency**

The BPMA may determine that a CA is not complying with its obligations set forth in this CP or the respective MOA. When such a determination is made, the BPMA may suspend operation of the BBCA (in the case where the BBCA is the non-compliant CA), or may direct the Boost Operational Authority to cease interoperating with the affected Entity Principal CA (e.g., by revoking the Certificate that the BBCA had issued to the Entity Principal CA), or may direct that other corrective actions be taken which allow interoperation to continue.

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

The compliance auditor shall note the discrepancy;

The compliance auditor shall notify the Entity of the discrepancy. The Entity shall notify the BPMA promptly;

The party responsible for correcting the discrepancy shall determine what further notifications or actions are necessary pursuant to the requirements of this CP and the MOA, 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 BPMA may decide to halt temporarily operation of the BBCA, to revoke a Certificate issued by the BBCA, or take other actions it deems appropriate. The BPMA shall develop procedures for making and implementing such determinations.

## **8.6 Communication of Results**

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

## **9 OTHER BUSINESS AND LEGAL MATTERS**

### **9.1 Fees**

#### **9.1.1 Certificate Issuance and Renewal Fees**

The BBCA and Entity CAs are entitled to charge for the issuance, management, rekey and renewal of any issued Certificates.

#### **9.1.2 Certificate Access Fees**

There shall be no fees charged by Boost Aerospace or any Entity PKI for any access associated with Relying Party access to Certificates in any Repository.

#### **9.1.3 Revocation or Status Information Access Fees**

There shall be no fees charged by Boost Aerospace or any Entity PKI for any access associated with Relying Party access to revocation or status information.

#### **9.1.4 Fees for Other Services**

Entity CAs may charge for other services. Boost Aerospace will set a fee schedule outlining the charges to Entity CAs for:

- Policy Mapping; and
- KRPS compliance.

#### **9.1.5 Refund Policy**

No Stipulation

## **9.2 Financial Responsibility**

### **9.2.1 Insurance Coverage**

Boost Aerospace and Entity CAs shall maintain reasonable levels of insurance coverage as required by applicable laws.

### **9.2.2 Other Assets**

Boost Aerospace and Entity CAs shall maintain sufficient financial resources to maintain operations and fulfill their respective obligations under this CP and applicable MOAs.

### **9.2.3 Insurance or Warranty Coverage for End-Entities**

No Stipulation

### **9.3 Confidentiality of Business Information**

Subscribers acknowledge that any information made public in a Certificate is deemed not private. In that respect, Certificates, OCSP responses, CRLs and personal or corporate information appearing in them and in public directories are not considered as private or confidential.

Personal and corporate information, which does not appear in Certificates and in public directories, held by a CA or an RA is considered confidential and shall not be disclosed by the CA or RA. Unless required by law or court order, any disclosure of such information requires Subscriber's written prior consent.

The treatment of confidential business information provided to external PKIs in the context of submitting an application for cross certification will be in accordance with the terms of the agreements entered into between the applicable entity and Boost Aerospace.

Each CA shall maintain the confidentiality of confidential business 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 the CA treats its own most confidential information.

### **9.4 Privacy of Personal Information**

For the purposes of the PKI related services, Boost Aerospace may collect, store, or process personally identifiable information. Any such use or disclosure shall be in accordance with applicable laws and regulations, specifically the European Data Protection Act and the Boost Aerospace Privacy Policy which is published at: [FIXME: URL OF DOCUMENT](#)

Entity CAs shall develop a Privacy Policy, and stipulate in their CP or a document referenced in their CP how they protect any personally identifiable information they collect.

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

### **9.5 Intellectual Property Rights**

#### **9.5.1 Property Rights in Certificates and Revocation Information**

Subject to any agreement between Boost Aerospace and the Entity CA, the Entity CA shall retain all intellectual property rights in and to the Certificates and revocation information that they issue. Entity CAs shall grant permission to reproduce and distribute Certificates, and/or use Revocation or Certificate status information on a non-exclusive, royalty-free basis, provided they are reproduced in full and that use of said Certificates is subject to a memorandum of agreement or equivalent contractual mechanism between the Entity CA, and their Subscribers and Relying Parties.

### **9.5.2 Property Rights in the CPS**

Boost Aerospace asserts that it owns and/or has licensed all Intellectual Property rights to this CP and related CPS. Furthermore, Boost Aerospace reserves all Intellectual property rights in this CP to be granted to any Licensor at its discretion in conjunction with any Memorandum or Agreement or equivalent contractual mechanism expressing such a license.

### **9.5.3 Property Rights in Names**

The Certificates may contain copyrighted material, trademarks and other proprietary information, and no commercial exploitation or unauthorised use of the material or information in or via the Certificates is permitted, except as may be provided in this CP or in any applicable agreement. In the event of any permitted use or copying of trademarks and/or copyrighted material, no deletions or changes in proprietary notices shall be made without written authorisation from the owner.

### **9.5.4 Property Rights in Keys**

Key pairs corresponding to Certificates of cross-certified CAs and Subscribers are the property of the cross-certified CAs and Subscribers that are the respective subjects of these Certificates, subject to the rights of Subscribers regardless of the physical medium within which they are stored and protected. Such persons retain all Intellectual Property Rights in and to these Key Pairs. Notwithstanding the foregoing, the BBKA Public Keys and self-signed Certificates, are the property of Boost Aerospace.

## **9.6 Representations and Warranties**

### **9.6.1 CA Representations and Warranties**

#### **9.6.1.1 Boost Bridge Certification Authority**

Boost Aerospace represents that, to be best of its knowledge:

- All Certificates issued and Revocation services provided, including CRLs issued, and OCSP responses, meet all material requirements of this CP and conforms to the applicable CPS in all material aspects; and
- the BBKA Repository is maintained in conformity with this CP and the applicable CPS in all material aspects; and
- There are no material misrepresentations of fact in any Cross-Certificates known to or originating from Boost Aerospace; and
- There are no errors in the information in any Cross-Certificate that were introduced by Boost Aerospace as a failure to exercise reasonable care in managing the Certificate application or creating the Certificate.

Contractual agreements discussed elsewhere in this section may include additional representations and warranties.

### **9.6.1.2 Entity Signing and/or Cross-Certified CAs**

All Cross-Certified and/or Signing Entity CAs represent and warrant that:

- There are no material misrepresentations of fact in the Cross-Certificates known to or originating from the entity approving the Cross Certification Applications or issuing the Cross-Certificates; and
- There are no errors in the information in the Cross-Certificate that were introduced by the entity approving the Cross Certification Application or issuing the Cross-Certificate as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate; and
- Their CA signing key is protected and that no unauthorised person has ever had access to the Private Key; and
- All representations made by the Signing CA or Cross-Certified CA in the applicable agreements are true and accurate; and
- All information supplied by the Subscriber in connection with, and/or contained in the Certificate has been duly verified; and
- The Certificate is being used exclusively for authorised purposes, consistent with this and any other applicable CP or CPS.

### **9.6.2 Subscriber Agreement**

An Entity CA shall require the Subscribers to sign a document containing the requirements the Subscriber shall meet respecting protection of the Private Key and use of the Certificate before being issued the Certificate. Subscribers shall agree to the following:

- Accurately represent themselves in all communications with the PKI authorities; and
- Protect their Private Keys at all times and prevent them from unauthorised access in accordance with this policy, as stipulated in their Subscriber agreement; and
- Promptly notify the appropriate CA upon suspicion of loss or compromise of their Private Keys. Such notification shall be made directly or indirectly through mechanisms consistent with this CP; and
- Abide by all the terms, conditions, and restrictions levied on the use of their Private Keys and Certificates, as set forth in this CP and the Subscriber agreement; and
- Use Certificates provided by the Entity CA only for authorised and legal purposes in accordance with the Entity CP; and
- Comply with all export laws and regulations for dual use goods as may be applicable, as relates to the usage and transport of keys, Certificates and algorithms mandated by this CP; and
- Cease to use such issued Certificates if they become invalid and remove them from any applications and/or devices they have been installed on.

PKI Sponsors (as described in section 5.2.1.4) shall assume the obligations of Subscribers for the Certificates associated with their components.

### **9.6.3 Relying Party**

Parties who rely upon Certificates issued under this policy shall:

- Only accept the use of the Certificate for the purposes indicated in the Certificate keyUsage and extendedKeyUsage extensions; and
- Verify the validity of the of said Certificate, using the procedures described in [RFC5280], prior to any reliance on such Certificate; and
- Establish trust in the CA who issued the Certificate by the methods outlined elsewhere in this CP, and using the path validation algorithm outlined in [RFC5280]; and
- Preserve the original signed data, the applications necessary to read and process that data, and the cryptographic applications needed to verify the digital signatures on that data for as long as it may be necessary to verify the signature on that data.

### **9.6.4 Representations and Warranties of Affiliated Organizations**

Affiliated Organizations shall authorize the affiliation of Subscribers with the organization, and shall inform the CA of any severance of affiliation with any current Subscriber.

### **9.6.5 Representations and Warranties of Other Participants**

No Stipulation

## **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, ENTITY 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 BOOST AEROSPACE AND ITS CUSTOMERS UNDER SEPARATE AGREEMENTS, (A) CERTIFICATES ISSUED BY THE BOOST AEROSPACE PKI ARE PROVIDED "AS IS", AND BOOST AEROSPACE, 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 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 BOOST AEROSPACE CERTIFICATES, ANY SERVICES PROVIDED BY BOOST AEROSPACE, OR THE VALIDATION OF ANY DIGITAL SIGNATURES LIES WITH THE APPLICABLE PARTICIPANT.

### **9.8 Limitations of Liabilities**

The liability and/or limitation thereof of Boost Aerospace to any Entity CA to which Boost Aerospace issues Certificates shall be set forth in the MOA between Boost Aerospace and that Entity CA.

OTHER THAN THE ABOVE DESCRIBED LIMITATIONS OF LIABILITY, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL BOOST AEROSPACE BE LIABLE FOR ANY INDIRECT DAMAGES OF ANY KIND, INCLUDING CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE, ANY COSTS, EXPENSES, OR LOSS OF PROFITS, OR OTHER DAMAGES WHATSOEVER ARISING OUT OF OR RELATED TO THIS CP, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO EVENT SHALL BOOST AEROSPACE BE LIABLE FOR ANY USAGE OF CERTIFICATE THAT EXCEEDS THE LIMITATIONS OF USAGE STATED UNDER THIS CP OR THAT IS NOT IN COMPLIANCE WITH THIS CP AND ASSOCIATED CPS.

BOOST AEROSPACE SHALL NOT BE LIABLE FOR ANY DAMAGE ARISING FROM THE COMPROMISE OF A SUBSCRIBER'S PRIVATE KEY OR ANY LOSS OF DATA.

THE TOTAL, AGGREGATE LIABILITY OF BOOST AEROSPACE ARISING OUT OF OR RELATED TO THIS CP SHALL BE LIMITED TO DIRECT DAMAGES ACTUALLY INCURRED, UP TO THE GREATER OF:

(A) THE AMOUNTS ACTUALLY PAID TO BOOST AEROSPACE UNDER THIS CP BY THE PARTY CLAIMING SUCH DAMAGES DURING THE TWELVE MONTHS IMMEDIATELY PRECEDING THE EARLIEST EVENT(S) GIVING RISE DIRECTLY TO THE LIABILITY OR

(B) TEN THOUSAND DOLLARS (\$10,000 USD).

THE TOTAL, AGGREGATE LIABILITY OF THE BOOST AEROSPACE BRIDGE CA ARISING OUT OF OR RELATED TO IMPROPER ACTIONS BY THAT CA SHALL BE LIMITED TO ONE THOUSAND DOLLARS (\$1,000 USD) PER TRANSACTION AND THE TOTAL LIABILITY OF BOOST AEROSPACE SHALL NOT EXCEED A MAXIMUM OF ONE MILLION DOLLARS (\$1 MILLION USD) IN AGGREGATE.

## **9.9 Indemnities**

### **9.9.1 Indemnification Customer CAs**

To the extent permitted by applicable law, each Entity CA shall indemnify Boost Aerospace 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 any Certificates issued by Boost Aerospace, including, without limitation, for:

- Falsehood or misrepresentation of fact by the Entity CA in the applicable contractual agreements; and
- Failure by the Entity 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; and
- The Entity CA's failure to protect the Entity 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 Entity CA private key; and
- The Entity CA's 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 between Boost Aerospace and an Entity CA that is a customer of Boost Aerospace may include additional indemnity obligations, but these would not apply to cross-certified CAs that are not customers of Boost Aerospace.

### **9.9.2 Indemnification by Relying Parties**

To the extent permitted by applicable law, each Relying Party shall indemnify Boost Aerospace 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 use of or reliance by Relying Party on any Certificates issued by Boost Aerospace, 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); and
- The Relying Party's unreasonable reliance on a Certificate, under the circumstances; and
- 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 Boost Aerospace and a Relying Party may include additional indemnity obligations, but these would not apply to relying parties that are not customers of Boost Aerospace.

## **9.10 Term and Termination**

### **9.10.1 Term**

This CP and any amendments thereto, becomes effective upon ratification by the Boost PMA and publication as a PDF document at the following location:

**FIXME: NEED URL**

There is no specified term or limitation thereon to this CP.

### **9.10.2 Termination**

While this CP may be amended from time to time, it shall remain in force until replaced by a newer version or explicitly terminated by a resolution of the Boost Aerospace Board of Directors. For purposes of clarity, termination of any Memoranda of Agreement shall not operate as a termination of this CP unless this CP is explicitly terminated by a separate resolution of the Boost Aerospace Board of Directors.

### **9.10.3 Effect of Termination and Survival**

Upon termination of this CP, CAs cross certified with Boost Aerospace 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 and termination or expiration of this CP: 2.1.1, 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**

All parties mentioned herein will use the methods specified in the respective agreements between the parties to communicate and/or deliver any relevant notices.

Notices and Communication to Relying Parties or other parties for whom an explicit agreement does not exist shall be by commercially reasonable methods, taking into account the criticality and subject matter of the communication.

## **9.12 Amendments**

### **9.12.1 Procedure for Amendment**

The BPMA shall review the CP and CPS at least once every year. Additional reviews may be enacted at any time at the discretion of the BPMA.

If the BPMA wishes to recommend amendments or corrections to the CP or CPS, such modifications shall be circulated to appropriate parties identified by the BPMA (including, without limitation, Entity CAs). Comments from such parties will be collected and incorporated into the respective document by the BPMA as described in the [BPMA Charter]. The [BPMA Charter] shall describe the manner in which such comments and amendments are accepted.

Notwithstanding the foregoing, if Boost Aerospace believes that material amendments to the CP are necessary immediately to stop or prevent a breach of the security of Boost Aerospace, they shall be entitled to make such amendments effective immediately upon publication in the Repository. Boost Aerospace shall use commercially reasonable efforts to immediately notify Entity CAs of such changes.

#### **9.12.2 Notification Mechanism and Period**

Errors and anticipated changes to the CP and CPS resulting from reviews shall be published publicly online. The location of the most up to date copy of the CP shall be described in the CPS, and clearly communicated on the Boost Aerospace web site.

In addition, changes are communicated by the OA Manager to every Boost Aerospace Customer via a designated point of contact, including a description of the change.

This CP and any subsequent changes shall be made publicly available within seven days of approval.

#### **9.12.3 Circumstances under Which OID Must be Changed**

Certificate Policy OIDs shall be changed if the BPMA determines that a change in the CP materially affects the level of assurance provided.

### **9.13 Dispute Resolution Provisions**

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

#### **9.13.1 Disputes among Boost Aerospace and Customers**

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

#### **9.13.2 Alternate Dispute Resolution Provisions**

In case of any dispute or disagreement between two or more participants arising out of or related to this CP, the Disputing Parties will use their best efforts to settle the dispute or disagreement through mediation or good faith negotiations following notice from one disputing party to the other. If the dispute is not successfully resolved by negotiation between the entities or the parties within sixty (60) days following the date of such notice, it shall be settled by final and binding arbitration before a single arbitrator knowledgeable in the information technology industry in accordance with the then existing Rules of Conciliation and Arbitration of the International Chamber of Commerce (ICC). The place of arbitration shall be defined in the relevant agreement between contracting parties. In the absence of such agreement, the place of arbitration shall be **TO BE DECIDED**.

This provision does not limit the right of a party to obtain other recourse and relief under any applicable law for disputes or disagreements that do not arise out of or which are not related to this CP.

## **9.14 Governing Law**

**TO BE COMPLETED**

## **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.

Parties agree to conform to applicable laws and regulations.

## **9.16 Miscellaneous Provisions**

### **9.16.1 Entire Agreement**

No stipulation

### **9.16.2 Assignment**

Except as otherwise provided under the applicable agreements, 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, except that Boost Aerospace may assign and delegate this CP to any party of its choosing.

### **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**

Boost Aerospace 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, natural disasters, fire, epidemic, flood, earthquake, riot, war, failure of equipment, failure of telecommunications lines, lack of Internet access, sabotage, and governmental action or any unforeseeable events or situations.

**BOOST AEROSPACE 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 BOOST AEROSPACE.**

## **9.17 Other Provisions**

No stipulation

## 10 Certificate Profiles

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

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

First entries in the caIssuers field of the AIA extension and CRL DP shall point to a resource that is publicly available.

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

For dc and e-mail address attribute values: All dc attribute values shall be encoded as IA5 string.

Certificate fields must not be listed in a predictable manner, in order to increase the difficulty of a cryptographic attack attempt.

Certificate Serial Numbers must not be assigned in a predictable manner, in order to increase the difficulty of a cryptographic attack attempt.

CAs may issue partitioned CRL as long as the CRLs are not indirect CRL, are not partitioned by reason code, and CRL DP and Issuing Distribution Point do not assert name relative to issuer. If the Entity PKI provides OCSP services for a CA, that CA must also issue a full and complete CRL (i.e., a CRL without Issuing Distribution Point extension) for the use by the OCSP Responder.

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

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



## 10.1 Boost Bridge CA to Principal CA

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} for Certificates issued before 1/1/2014 or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	<b>TO BE DECIDED</b>
Validity Period	Expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 CA DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	2048 bit modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	Value
Authority Key Identifier	c=no; Octet String (same as in PKCS-10 request from the CBCA)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request from the PCA)
Key Usage	c=yes; keyCertSign, cRLSign, DigitalSignature, nonRepudiation
Certificate Policies	c=no; Applicable policies from section 7
Policy Mapping	c=no; Applicable policy mappings according to the MOA
Basic Constraints	c=yes; cA=True; path length constraint optional <sup>5</sup>
Name Constraints <sup>6</sup>	c=yes; permitted subtrees for DN, RFC-822, and DNS name forms
Policy Constraints	c=no; inhibitPolicyMapping skipCerts = 0
Authority Information Access	c=no; id-ad-caIssuers access method entry containing HTTP URL for .p7c file containing Certificates issued to BBBCA
CRL Distribution Points	c=no; LDAP and/or HTTP URL of CRL location
Inhibit anyPolicy	c=no; skipCerts = 0

<sup>5</sup> Path length constraint must be present when name constraints is not used.

<sup>6</sup> Name constraint extension may be omitted with BPMA approval, e.g., when the PCA includes service providers. BPMA may decide to assert a subset of or additional name forms in special circumstances.

## 10.2 Principal CA to Boost Bridge CA

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} for Certificates issued before 1/1/2014 or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 CA DN as specified in Section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049
Subject Distinguished Name	<b>TO BE DECIDED</b>
Subject Public Key Information	2048 bit modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	Value
Authority Key Identifier	c=no; Octet String (same as in PCA PKCS-10 request to the CBCA)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request from the CBCA)
Key Usage	c=yes; keyCertSign, cRLSign, DigitalSignature, nonRepudiation
Certificate Policies	c=no; Applicable policies from section 7 of Entity CA CP
Policy Mapping	c=no; Applicable policy mappings as described in the MOA
Basic Constraints	c=yes; cA=True; path length constraint absent
Name Constraints	c=yes; optional, excluded subtrees: Name forms as determined by the Entity PMA
Authority Information Access	c=no; id-ad-caIssuers access method entry containing HTTP URL for .p7c file containing Certificates issued to PCA
CRL Distribution Points	c = no;
Inhibit anyPolicy	c=no; skipCerts = 0

### 10.3 Self-Signed Root Certificate (also called Trust Anchor)

<b>Field</b>	<b>Value</b>
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or Certificates issued before 1/1/2014 or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 CA DN as specified in Section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 CA DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	2048 bit modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256WithRSAEncryption {1 2 840 113549 1 1 11}
<b>Extension</b>	<b>Value</b>
Subject Key Identifier	c=no; Octet String (same as in PCA PKCS-10 request to the CBCA)
Key Usage	c=yes; keyCertSign, cRLSign, DigitalSignature, nonRepudiation
Basic Constraints	c=yes; cA=True; path length constraint absent

## 10.4 Intermediate or Signing CA Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} for Certificates issued before 1/1/2014 or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 Subject CA DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	2048 bit modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	Value
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request from the subject CA )
Key Usage	c=yes; keyCertSign, cRLSign, DigitalSignature, nonRepudiation
Certificate Policies	c=no; Applicable policies as per section 7 of Entity CA CP
Basic Constraints	c=yes; cA=True; path length constraint absent or value per Issuer PKI
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA
CRL Distribution Points	c = no;

## 10.5 Subscriber Identity Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} for Certificates issued before 1/1/2014 or sha256WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	No longer than 3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	2048 bit modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	Value
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA per RFC 3280 method 1 or other method)
Key Usage	c=yes; digitalSignature
Extended Key Usage	optional, c=no; at least Client Authentication {1.3.6.1.5.5.7.3.2}
Certificate Policies	c=no; Applicable policies
Subject Alternative Name	c=no; recommended to include email address of Subscriber as rfc822 email address, other name forms optional
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder when provided by Entity CA
CRL Distribution Points	c = no;

## 10.6 Subscriber Signature Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} for Certificates issued before 1/1/2014 or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	No longer than 3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	2048 bit modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	Value
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; digitalSignature, nonRepudiation
Extended Key Usage	optional, c=no; at least has Secure Email {1.3.6.1.5.5.7.3.4}
Certificate Policies	c=no; Applicable policies
Subject Alternative Name	c=no; RFC822 email address (required)
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder when provided by Entity CA
CRL Distribution Points	c = no;

## 10.7 Subscriber Encryption Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} for Certificates issued before 1/1/2014 or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	No longer than 3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	2048 bit modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	Value
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; keyEncipherment (required), dataEncipherment (optional)
Certificate Policies <sup>7</sup>	c=no; Applicable Certificate policies
Subject Alternative Name	c=no; RFC822 email address (required)
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder when provided by Entity CA
CRL Distribution Points	c = no;

<sup>7</sup> It is recommended that only "software" assurance levels are used, since escrowed keys are inherently only as secure as the software tokens (PKCS#12 containers) to which they are recovered.

## 10.9 Code Signing Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} for Certificates issued before 1/1/2014 or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	2048 bit modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	Value
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate )
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; nonRepudiation, digitalSignature
Extended key usage	c=yes; { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) id-kp(3) id-kp-codesigning(3) }
Certificate Policies	c=no; Applicable policies
Subject Alternative Name	DN of the person controlling the code signing private key
CRL Distribution Points	c = no;
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder when provided by Entity CA

## 10.10 Device or Server Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} for Certificates issued before 1/1/2014 or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP cn={ Host URL   Host IP Address   Host Name }
Subject Public Key Information	2048 bit modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	Value
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate )
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; keyEncipherment, digitalSignature
Extended Key Usage	optional; c=no; at least contains Server Authentication
Certificate Policies	c=no; Applicable policies
Subject Alternative Name	c=no; always present, one or more Host URL   IP Address   Host Name
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder when provided by Entity CA
CRL Distribution Points	c = no; always present

## 10.11 OCSP Responder Certificate

The following is the OCSP Responder Certificate profile which must be used. This profile assumes that the OCSP Responder Certificate is issued by the same CA using the same key as the Subscriber Certificate. For compatibility, no other trust model may be used.

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} for Certificates issued before 1/1/2014 or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	No longer than one month from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 OCSP Responder (subject) DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	2048 bit modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	Value
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate )
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; nonRepudiation, digitalSignature
Extended key usage	c=yes; id-kp-OCSPSigning {1 3 6 1 5 5 7 3 9}
Certificate Policies	c=no; Applicable policies
Subject Alternative Name	HTTP URL for the OCSP Responder
No Check id-pkix-ocsp-nocheck; {1 3 6 1 5 5 7 48 1 5}	c=no; Null
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to issuing CA

## 10.12 CRL Format

### 10.12.1 Full and Complete CRL

Field	Value
Version	V2 (1)
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
thisUpdate	expressed in UTCTime until 2049
nextUpdate	expressed in UTCTime until 2049 ( $\geq$ thisUpdate + CRL issuance frequency)
Revoked Certificates list	0 or more 2-tuple of Certificate serial number and revocation date (in Generalized Time)
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
CRL Extension	Value
CRL Number	c=no; monotonically increasing integer (never repeated)
Authority Key Identifier	c=no; Octet String (same as in Authority Key Identifier field in Certificates issued by the CA)
CRL Entry Extension	Value
Reason Code	c=no; optional, must be included when reason code = key compromise or CA compromise

### 10.12.2 Distribution Point Based Partitioned CRL

Field	Value
Version	V2 (1)
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
thisUpdate	expressed in UTCTime until 2049
nextUpdate	expressed in UTCTime until 2049 ( $\geq$ thisUpdate + CRL issuance frequency)
Revoked Certificates list	0 or more 2-tuple of Certificate serial number and revocation date (in Generalized Time)
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
CRL Extension	Value
CRL Number	c=no; monotonically increasing integer (never repeated)
Authority Key Identifier	c=no; Octet String (same as in Authority Key Identifier field in Certificates issued by the CA)

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

## 10.13 OCSP Request Format

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

## 10.14 OCSP Response Format

Field	Value
Response Status	As specified in RFC 2560
Response Type	id-pkix-ocsp-basic {1 3 6 1 5 5 7 48 1 1}
Version	V1 (0)
Responder ID	Octet String (same as subject key identifier in Responder Certificate)
Produced At	Generalized Time
List of Responses	Each response will contain Certificate id; Certificate status <sup>8</sup> , thisUpdate, nextUpdate <sup>9</sup> ,
Responder Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256WithRSAEncryption {1 2 840 113549 1 1 11}
Certificates	Applicable Certificates issued to the OCSP Responder
<b>Response Extension</b>	<b>Value</b>
Nonce	c=no; Value in the nonce field of request (required, if present in request)
<b>Response Entry Extension</b>	<b>Value</b>
None	None

---

<sup>8</sup> If the Certificate is revoked, the OCSP Responder shall provide revocation time and revocation reason from CRL entry and CRL entry extension.

<sup>9</sup> The OCSP Responder shall use thisUpdate and nextUpdate from the current CA CRL.

**Appendix A: Bibliography**

**Appendix B: Glossary**