X.509 Certificate Policy for the Federal Aviation Administration (FAA) Non-Person Entity (NPE) Certification Authority (CA) Version 1.5

January 15, 2026

FAA PMA Co-Chair:

Signature: Signed by: Jonathan Beams

Signer Name: Jonathan Beams
Signing Reason: I approve this document
Signing Time: 1/20/2026 | 3:21:37 AM PST
325A74DA56874F45BFDB8CE83458EF31

Name: Jonathan Beams

FAA SUPVY IT SPECIALIST - AFN

Revision History

Document Version	Document Date	Revision Details
.92	09/30/21	ICAO Doc 10169 Manual on Aviation Common Certificate Policy Baseline
.93	10/30/21	FAA Draft Baseline
.94	3/30/22	FAA Draft Updates
.95	3/30/23	FAA Draft Updates
.96	11/30/23	FAA Draft Updates
.97	01/18/2023	FAA Draft Updates
.98	04/02/2024	FAA Draft Updates
.99	04/24/2024	CPWG UPDATES
1.0	6/11/2024	Official release
1.1	7/30/2024	Updates to address WebTrust Control
1.2	6/23/2025	Update to OID
1.3	07/07/2025	Update to align with FAA NPE CP 1.2
1.4	08/19/2025	Update to align with ICAO ACCP
1.5	01/15/2025	Update Section 1.5.1 Contact Person

Contents

1. INTRODUCTION

This Public Key Infrastructure (PKI) Certificate Policy (CP) defines multiple Assurance Levels for Certificates issued to Non-Person Entities (NPEs) for use by the Federal Aviation Administration (FAA) NPE Root, Principal, and Subordinate Certification Authorities (CA) to facilitate interoperability between the CAs and external Entity PKI domains.

The level of assurance (LOA) not only refers to the strength of the identity Binding between the Public Key and the NPE whose subject name is cited in the Certificate, but also to how well the Certificate Owner of the NPE 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 secure the PKI which was used to produce the Certificate and (if appropriate) deliver the Private Key to the Subscriber is. This facilitates trust decisions and interoperability across the Aviation Community.

This Certificate Policy defines several policies applicable to the use of digital Certificates for authentication, integrity (through digital signatures) and encryption to provide digital Certificates to NPE End-Entities.

The policies represent the following Assurance Levels for Public Key Certificates:

- *LowDevice*
- *Low-TSPMediatedSignature*
- *MediumDevice*
- *Medium-TSPMediatedSignature*
- *MediumDeviceHardware*

This policy covers the FAA Root, Principal and Subordinate CAs. The CAs may cross certify with other PKI domains to allow interoperation with other Enterprises required for the business of FAA, its Business Units, affiliated companies, and customers. The LOA is reflected in Object Identifiers (OIDs).

Any use of or reference to this CA CP outside the purview of the CA is completely at the Relying Party's Risk. An Entity shall not assert the CA CP OID in any Certificates the Entity CA issues, except in the *policyMappings* extension establishing an equivalency between a CA OID and an OID in the Entity CA's CP.

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

1.1 OVERVIEW

A Certificate issued in accordance with this Certificate Policy (CP) conveys within the Aviation Community a level of digital identity assurance associated with the Subject of the Certificate. A *Low* or *Medium* identity level of assurance may be conveyed. The term "identity level of assurance" used in this CP means how certain a Relying Party (RP) can be of the identity Binding between the Public Key and the NPE whose subject name is cited in the Certificate. In addition, it also reflects how certain the Relying Party can be that the NPE Certificate Owner 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 Subscriber, performs its task. A Certificate Subject may be an organization, a server, application, information artifacts, or device (including ground systems, aircraft and aircraft avionics), subject to the rules concerning each described in this CP. The type and level of identity assurance conveyed are represented in the OID structure in Section 1.2.

The identity of the Subscriber, whether a Person or NPE, is confirmed via Out-of-Band communications.

Certificate Policy (CP)

FAA Certificates contain one or more registered Certificate policy Object Identifiers (OID), which may be used by a Relying Party to decide whether a Certificate is trusted for a particular purpose. The OID corresponds to a specific level of assurance established by this CP, which shall be available to RPs. Each Certificate issued by the FAA shall assert the appropriate level of assurance in the *CertificatePolicies* [1] extension.

Relationship between the CP and CPS

A CP states what assurance can be placed in a Certificate issued by the Certificate Authority (CA). The Certification Practice Statement (CPS) states how the CA establishes that assurance. A CPS shall be more detailed than the CP with which it aligns.

Relationship between the FAA NPE CA CP *the other PKI domains' CPs*

The FAA PKI Policy Management Authority (PMA) shall map Root, Bridge, or Principal CA CP(s) to one or more of the levels of assurance in the FAA CA CP. The relationship between these CPs and the FAA CA CP is asserted in CA Certificates issued by the FAA CA in the policyMappings extension.

Scope

The CAs exists to facilitate trusted electronic business transactions internally and externally across industry, State, and international boundaries.

The Root CA shall issue CA Certificates only to Principal and Subordinate CAs approved by the PMA.

Principal and Subordinate CAs may issue Certificates to NPEs at any Assurance Level consistent with the CP.

Within this document, the term CA, when used without qualifier, shall refer to any Certification Authority subject to the requirements of this CP.

The scope of this CP, in terms of Subscriber Certificate types, is limited to those listed in Section 10.

Interaction with PKIs External to FAA

The FAA shall extend trust interoperability only when it is beneficial to the FAA lines of business and Staff offices.

1.2 DOCUMENT NAME AND IDENTIFICATION

This document is called the FAA Non-Person Entity Certificate Policy (CP).

[1] PKI data objects, e.g., *CertificatePolicies*, use the Abstract Syntax Notation One (ASN.1)- like syntax defined in RFC 5280 Appendix A. These are represented in *italics* in this document.

There are five (5) levels of assurance Policy OIDs defined in Table 1 - FAA Certificate Policy Level of Assurance OIDs and OID Structure, in this Certificate Policy for use by the FAA line of business (LOBs); which include A-Operating Environment (OE) (AIT), Research and Development (RD)-OE (ANG), Mission Critical (MC)-OE (NAS) and Mission Essential (ME)-OE (NAS), (the "FAA LOBs").

Each Assurance Level is uniquely represented by an "object identifier" (OID), which is asserted in each Certificate issued by the CAs that complies with the policy stipulations under this CP.

See Section 1.4.1, Appropriate Certificate Uses, provides the definition of applicability for each.

The FAA level of assurance policy OIDs are a sub-assignment of International Civil Aviation Organization (ICAO) OIDs registered in the Internet Assigned Numbers Authority (IANA) OID Repository. ICAO DOC 9880, Technical Specifications for Aeronautical Telecommunications Network (ATN) using International Organization for Standardization (ISO) / Open System Interconnection (OSI) Standards and Protocols, contains the ICAO sub-assignments and this CP documents the further sub-assignments.

Table 1 - FAA Certificate Policy Level of Assurance OIDs and OID Structure

OID Structure Assignments		
iso	1	1
identified-organization	3	1.3
ICAO	27	1.3.27
security	16	1.3.27.16
PKI	1	1.3.27.16.1
Common Security Requirements	1	1.3.27.16.1.1
X.509 CP	0	1.3.27.16.1.1.0
Level of Assurance OIDS		
LowDevice	2	1.3.27.16.1.1.0.2
Low-TSPMediatedSignature	3	1.3.27.16.1.1.0.3
MediumDevice	5	1.3.27.16.1.1.0.5
Medium-TSPMediatedSignature	6	1.3.27.16.1.1.0.6
MediumDeviceHardware	8	1.3.27.16.1.1.0.8

Other CP OIDs		
FAA CP	1	1.3.6.1.4.1.44109.0.1

The requirements associated with the *mediumDevice* policy are identical to those defined for the *Medium* Assurance policy with the exception of identity proofing, re-key, and Activation Data. The requirements associated with the *mediumDevice*Hardware policy are identical to those defined for the *Medium Hardware* Assurance policy with the exception of identity proofing, re-key, and Activation Data.

In this CP when referring to the Level of Assurance OIDs, the term "Device" is defined as a Non-Person Entity (NPE), i.e., an entity with a digital identity that acts in cyberspace but is not a human actor. This can include Organizations, hardware devices, software applications, and information artifacts.

End-Entity Certificates issued to "NPEs" will not assert policies mapped to *LowDevice*, *MediumDevice, and MediumDeviceHardware* policies to protect the FAA from publishing the method of storing the end entity certificate private key. All other policies defined in this document should be reserved for human Subscribers when used in End-Entity Certificates.

The requirements associated with the *Medium* Hardware Assurance Level are identical to those defined for the *Medium* Assurance Level with the exception of Subscriber Cryptographic Module requirements. See Section 0

A Trust Service Provider (TSP) *Mediated Signature* OID is used in a Certificate where the Private Key is under the control of but not in the possession of the user, such as where the user's Private Key is in a hardware security module (HSM) in the possession of a Trust Service Provider.

1.3 FAA PKI PARTICIPANTS

The following paragraphs provide descriptions of roles relevant to the management administration and operation of the FAA A-OE, ME-OE, MC-OE and RD-OE PKI mission need operating environments. See FAA Order 1370.121 B, Tier 2, Appendix 2, Roles and Responsibilities and the PMA Charter.

FAA PKI Authorities

The FAA Public Key Infrastructure (PKI) Management Authority (PMA) is defined in FAA Order 1370.121B.

1.3.1.1 PKI Policy Management Authority (PMA)

The PMA is chartered by and under the authority of the FAA CSC. The members of the PMA are represented by the FAA LOBs stakeholders.

The PMA owns this policy and represents the interest of FAA. The PMA is responsible for:

- Authoring and maintaining this CP, including revisions,
- Reviewing and approving the CPS and any updates for consistency with the CP prior to Operational Authority (OA) signing of the CPS,
- Authoring and maintaining the methodology for cross-certification,

- Accepting applications from Entities desiring to interoperate with the FAA,
- Approving cross-certification of Entities, and
- After cross certification with an external CA, responsible for ensuring continued conformance of that external CA with applicable requirements as a condition for allowing continued interoperability using the FAA.

1.3.1.2 PKI Policy Working Group (WG)

The Working Group (WG) provides policy coordination and analysis services in support of the PMO, PMA, and OA. The members of the WG are represented by the FAA LOBs stakeholders.

The WG is responsible for the following:

- Analyzing and reviewing the CA CP and CPS and audit results.
- Analyzing change requests for this CP and the related CPS.
- Recommending CP and CPS Change requests to the PMA and OA.
- Performing analysis and coordination services according to the cross-certification methodology. The results of such services are reports and recommendations to the PMA and who makes approval decisions.
- Performing analysis and coordination services for incident handling, disaster recovery, change control, and business continuity scenarios.

1.3.1.3 FAA Operational Authority (OA)

The OA is the collection of FAA LOBs organization OAs that operate and maintain the CAs on behalf of FAA, according to this CP. The FAA Operations Authority (OA) is led by the Operational Authority Administrator (OAA), who is principally responsible for the proper operation of the NPE CA.

The OA Administrator is the individual within the A-OE, ME-OE, MC-OE and RD-OE Operational Authority who has principal responsibility for overseeing the proper operation of the CA infrastructure components, and who appoints individuals to other roles within the CA.

The Administrator is selected by and reports to the PMO.

The Administrator approves the issuance of Certificates to the other trusted roles operating the CAs.

1.3.1.4 Principal Certificate Authority (CA)

The Principal CA is the CA operated by the OA that is authorized by the PMA to create, sign, and issue Public Key Certificates to subscribers. As operated by the OA, the Principal CA is responsible for all aspects of the issuance and management of a Certificate including:

- Control over the Subject registration, identification and authentication process,
- Control over the Certificate issuance process,
- Publication of Certificates,
- Revocation of Certificates,
- Re-key of CA signing material and

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

A Principal CA is an Entity CA within a PKI that has been designated to cross-certify directly with the FAA CA (e.g., through the exchange of Cross-Certificates). The Principal CA issues either End-Entity Certificates or CA Certificates to other Entity or external party CAs, or both. Where the Entity operates a hierarchical PKI, the Principal CA is typically the Entity Root CA. Where the cross-certifying Entity operates a mesh PKI, the Principal CA may be any CA designated by the Entity for cross-certification with the FAA CA.

An Entity may request that the FAA CA cross-certify with more than one CA within the Entity; that is, an Entity may have more than one Principal CA. Additionally, this CP may refer to CAs that are “subordinate” to the Principal CA. The use of the term “Subordinate CA” (SCA) shall encompass any CA under the control of the Entity that has a Certificate issued to it by the Entity Principal CA or any CA subordinate to the Principal CA, whether or not the Entity employs a hierarchical or other PKI architecture.

1.3.1.5 Subordinate Certification Authorities (SCA)

A Subordinate CA shall be a CA which is not a Root CA and whose primary function is to issue Certificates to other CAs. Subordinate CAs may or may not issue Certificates to End-Entities.

A Signing CA shall be a CA whose primary function is to issue Certificates to End-Entities. A Signing CA does not issue Certificates to other CAs.

As operated by the Operational Authority, an Entity SCA shall be responsible for all aspects of the issuance and management of an End-Entity Certificate, as detailed in this CP, including:

- The control over the Registration process
- The identification and authentication process
- The Certificate issuance process
- The publication of Certificates
- The Revocation of Certificates and
- Ensuring that all aspects of the services, operations and infrastructure related to Certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP.

1.3.1.6 Root Certification Authority (RCA)

The FAA will operate one or more self-signed Root CAs which shall be called the RCA. The RCA shall issue and revoke Certificates to Signing CAs (PCAs and SCAs) upon authorization by the PMA. As operated by the Operational Authority, an RCA is responsible for all aspects of the issuance and management of a Certificate including:

- Control over the Registration process
- The identification and authentication process
- The Certificate issuance process
- Publication of Certificates
- Revocation of Certificates

- Re-key of RCA signing material and
- Ensuring that all aspects of the services, operations and infrastructure related to Certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP.

1.3.1.7 Time-Stamp Authority (TSA)

A TSA is an authority that issues and validates Trusted Timestamps. A TSA may be operated in conjunction with a CA or independent of a CA. Each FAA Operation Environment will describe requirements for authoritative time stamping of PKI transactions in the CPS that implements this CP.

1.3.1.8 Certificate Status Authority (CSA)

FAA PKIs must include an authority that provides status information about Certificates on behalf of a CA through online transactions. In particular, FAA PKIs must include Online Certificate Status Protocol (OCSP) responders to provide online status information. Such an authority is termed a CSA. The CSA must be identified in Certificates as an authoritative source for Revocation information, and the operations of that authority are considered within the scope of this CP. Examples of CSA that fall within the scope of this CP include:

- OCSP Servers that are identified in the authority information access (AIA) extension
- Server-based Certificate Validation Protocol (SCVP) Servers that validate paths or perform Certificate status checking
- When used by an OE CSA that uses OCSP Servers that are locally trusted, as described in RFC 6960, (MC-OE JO-1370.123 example) shall document FAA Relying party requirements in the CPS and other FAA Configuration Managed requirements documents such as NAS CCB approved Interface Requirements documents and COMM CCB Interface Control Documents

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

1.3.1.9 Administration Workstation

If access is required to administer CA and CSA equipment and/or associated Hardware Security Module (HSM) from a specific secure location outside the physical security perimeter of the CA, and CSA, it shall be done through an Administration Workstation. This device is considered to be a logical extension of the Secure Enclave in which the CA, Key Escrow System (KES and CSA) equipment reside and shall follow security requirements detailed at other sections of this CP.

Registration Authorities

1.3.1.10 Registration Authority (RA)

An RA shall be a Trusted Role that collects and verifies Subscriber identity and information for inclusion in the Subscriber’s Public Key certificate. An RA shall interact with the CA to enter and approve the Subscriber Certificate Request information. The Operational Authority (OA) shall act as the RA for the Root, Principal and Subordinate CAs. It shall perform its function in accordance with the relevant CA CPS approved by the PMA.

In all cases, an RA shall possess a Certificate of assurance level equal to or greater than that of the Certificate being issued, protected as described in Section 6.1.1 and Section 6.2.1.

Entity CAs shall designate their RAs. The requirements for RAs in FAA PKI are set forth in Section 5.2.2.4.

Subscribers

A Subscriber shall be the NPE to which a certificate is issued, and whose name appears as the Subject in a Certificate. The NPE shall have a human sponsor (Device Sponsor see section 1.3.3.4) who is responsible for carrying out human Subscriber duties.

Root CA Subscribers shall only include Entity PKI CA Operational Authority personnel and, when determined by the PMA, certain network or hardware devices such as Firewalls and routers when needed for PKI-infrastructure protection.

Principal and Subordinate CA Subscribers shall include hardware devices such as Firewalls, routers, Servers, and others having to operate and/or do business or act in any lawful capacity within the global air transport or aerospace community.

1.3.1.11 Affiliated Organizations

Subscriber Certificates may be issued in conjunction with an organization that has a relationship with the subscriber; this is termed affiliation. The organizational affiliation shall be indicated in a relative distinguished name in the subject field in the Certificate, and the Certificate shall be revoked in accordance with Section 4.9.1 when affiliation is terminated.

1.3.1.12 Non-Person Entity (NPE)

These are a broad class of physical and virtual entities which function on the network. NPEs use PKI authentication to validate their identity to other NPEs or be authenticated to by other NPEs or human Subscribers. Examples are workstations, guards and firewalls, routers, trusted database servers and other networked electronic components or applications that execute on one of these systems that must be authenticated. These components must be under the cognizance of humans called Device Sponsors who accept the certificate and are responsible for the correct protection and use of the associated private key.

PRACTICE-NOTE: *Generally, the Device Sponsor is a System Administrator or Operator who is responsible for the operations of an Entity system. In the case of an aircraft device, the Device Sponsor is an airline representative. The Device Sponsor is ultimately responsible to supply the CA with all identification data required for the Certificate issuance.*

1.3.3.3 Code Signer

A Code Signer is a NPE designated by an Organization as authorized to have and use a PKI Code Signing certificate.

1.3.3.4 Device Sponsors

A Device Sponsor is an individual who requests a Certificate on behalf of an NPE. The Device Sponsor asserts that the NPE shall use the key and Certificate in accordance with the Certificate Policy asserted in the Certificate.

Relying Parties (RP)

A Relying Party is an Entity that relies on the validity of the Binding of the Subscriber's name to a Public Key. A Relying Party may use a Subscriber’s Certificate to verify the Integrity of a digitally signed message, document or transaction, to identify the creator of a message document or transaction, or to negotiate session keys for the establishment of confidential communications with the Subscriber. The Relying Party shall be responsible for deciding whether or how to check the validity of the Certificate by checking the appropriate Certificate status information. A Relying Party may use information in the Certificate (such as Certificate policy identifiers) to determine the suitability of the Certificate for a particular use.

This CP makes no assumptions or limitations regarding the identity of Relying Parties. While Relying Parties are generally Subscribers, Relying Parties are not required to have an established relationship with the CA or an Entity CA.

Other Participants

1.3.1.13 Related Authorities and Additional Participants

The CAs may require the services of other security, community, auditors, and application authorities, such as compliance auditors and attribute authorities. If required, the CA/CPS shall identify the parties, define the services, and designate the mechanisms used to support these services.

1.3.1.14 Trusted Agent (TA)

The Trusted Agent is the representative of the subscriber (or collectively the LOB) that collects and verifies each Subscriber’s identity and information on behalf of an RA. Information shall be verified in accordance with Section 3.2 and communicated to the RA in a secure manner.

Trusted Agent shall not have access to the CA to enter or approve Subscriber information. See section 5.2.2 for more information.

1.3.1.15 Systems Administrator (SA)

An SA is a person authorized to perform operations on the RA systems that require privileged access.

1.3.1.16 Information System Security Officer (ISSO)

An ISSO is designated by the RA organization and is responsible for providing security services that support the RA operation.

1.3.1.17 Compliance Auditor

A compliance auditor performs compliance audits as specified in Chapter 8.

1.3.1.18 Applicability

The sensitivity of the information processed or protected using Certificates issued by CAs will vary significantly. Relying Parties shall evaluate the environment and the associated Threats and vulnerabilities and determine the level of Risk they are willing to accept based on the sensitivity or significance of the information. This evaluation is done by each Relying Party for each application and is not controlled by this CP.

To provide sufficient granularity, this CP specifies security requirements at various levels of assurance as listed in Section 1.2.

1.3.3.7 Factors in Determining Usage

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

1.3.3.8 Obtaining Certificates

Relying Party applications shall make their own arrangements for obtaining Subscriber Certificates; this can be done, for example, in the standard application protocols for Signature and Authentication Certificates.

1.4 CERTIFICATE USAGE

Appropriate Certificate Uses

To provide sufficient granularity, this CP specifies security requirements at multiple levels of assurance. The following table provides a brief description of possible appropriate uses for Certificates at each level of assurance defined in this CP. These descriptions are intended as guidance and are not binding. In their CPs, Entities may also wish to provide additional information concerning Assurance Levels including a brief and non-binding description of the applicability for applications suited to each level.

Table 2, Identity Assurance level Appropriate Certificate Uses

Assurance Level	**Applicability**
Low	This level is relevant to environments where Risks and consequences of data Compromise are low. Subscriber Private Keys are stored in software security module at this Assurance Level. Reserved for Human Subscribers. See section 3.2.3.2, Individual Subjects
LowDevice	This level is relevant to environments where Risks and consequences of data Compromise are low. Subscriber Private Keys are stored in software security module at this Assurance Level. Reserved for Non-Person Entity Subscribers. See section 3.2.3.1, NPE Subjects

Low-TSPMediated Signature	This level is relevant to environments where Risks and consequences of data Compromise are low. A Trust Service Provider (TSP) Mediated Signature OID is used in the Certificate where the Private key is under the control of but not in the possession of the user. See section 3.2.3.4, Individual Subject for TSP Mediated Signature Certificates Subscriber Private Keys may be stored in software security module at this Assurance Level. Reserved for Human Subscribers. See section 3.2.3.2, Individual Subject for TSP Mediated Signature Certificates
Medium	This level is relevant to environments where Risks and consequences of data Compromise are moderate. This may include transactions having substantial monetary value or Risk of fraud or involving access to private information where the likelihood of malicious access is substantial. Subscriber Private Keys may be stored in software security module at this Assurance Level. Reserved for Human Subscribers. See section 3.2.3.2, Individual Subjects
MediumDevice	This level is relevant to environments where Risks and consequences of data Compromise are moderate. This may include transactions having substantial monetary value or Risk of fraud or involving access to private information where the likelihood of malicious access is substantial. Subscriber Private Keys may be stored in software at this Assurance Level. The requirements associated with the *MediumDevice* policy are identical to those defined for the *Medium* Assurance policy with the exception of identity proofing, re-key, and Activation Data. Reserved for Human Subscribers. See section 3.2.3.2, Individual Subjects

MediumHardware	This level is relevant to environments where Risks and consequences of data Compromise are moderate. This may include transactions having substantial monetary value or Risk of fraud or involving access to private information where the likelihood of malicious access is substantial. Subscriber Private Keys must be stored in hardware security module at this Assurance Level. The requirements associated with the *Medium* Hardware Assurance Level are identical to those defined for the id-*Medium* Assurance Level with the exception of Subscriber Cryptographic Module requirements. See Section 6.2.1 Reserved for Non-Person Entity Subscribers. See section 3.2.3.4, NPE Subjects
MediumDeviceHardware	This level is relevant to environments where Risks and consequences of data Compromise are moderate. This may include transactions having substantial monetary value or Risk of fraud or involving access to private information where the likelihood of malicious access is substantial. Subscriber Private Keys must be stored in hardware security module at this Assurance Level. The requirements associated with the *MediumDeviceHardware* policy are identical to those defined for the *MediumHardware* Assurance policy with the exception of identity proofing, re-key, and Activation Data. Reserved for Non-Person Entity Subscribers. See section 3.2.3.1, NPE Subjects.
Medium-TSPMediated Signature	This level is relevant to environments where Risks and consequences of data Compromise are moderate. This may include transactions having substantial monetary value or Risk of fraud or involving access to private information where the likelihood of malicious access is substantial. A Trust Service Provider (TSP) Mediated Signature OID is used in the Certificate where the Private key is under the control of but not in the possession of the user. See section 3.2.3.4, Individual Subject for TSP Mediated Signature Certificates Subscriber Private Keys must be stored in hardware security module at this Assurance Level. Reserved for Human Subscribers. See section 3.2.3.4, Individual Subjects for TSP Mediated Signature Certificates

In addition to the above:

For CAs, Role-Based Code Signing Certificates, in which the role is clearly indicated to be the signature of Aircraft software/parts, are relevant to environments where software is to be loaded onto an aircraft system, the integrity of the software needs to be assured, and the source organization of the software needs to be identified. Subscriber private keys shall be stored in hardware at this Assurance Level. Such Certificates shall only be issued to Organizations and corporations.

> **PRACTICE-NOTE:** It is common practice in the Aviation Industry to indicate a parts signing Certificate by adding a designator in the Subject CN value e.g., Role LSAP Signer

Prohibited Certificate Uses

See Section 9.17.1 and 9.17.2 of this CP.

1.5 POLICY ADMINISTRATION

1.5.1 Organization administering the document

The PMA is responsible for all aspects of this CP.

1.5.2 Contact Person

Questions regarding this CP will be directed to FAA Certificate Questions and Problem Report.

Please send any comments to the above.

1.5.3 Person Determining CPS Suitability for the Certificate Policy

The term CPS is defined in the Internet RFC 3647, X.509 Public Key Infrastructure Certificate Policy and Certification Practice Statement Framework as: "A statement of the practices, which a Certification Authority employs in issuing Certificates." It is a comprehensive description of such details as the precise implementation of service offerings and detailed procedures of Certificate life-cycle management. It shall be more detailed than the corresponding Certificate Policy. In all cases, the Certification Practices Statement shall conform to the corresponding Certificate Policy.

The PMA is responsible for asserting whether the CA CPS conforms to this CP, substantiated by the audit report of an independent auditor or compliance analyst competent in the operations of a PKI. See Section 8 for further details.

1.5.4 Certificate Practice Statement Approval Procedures

The OA shall prepare and submit the CA CPS to the PMA for approval. If rejected, the identified discrepancies shall be resolved, and the CA CPS shall be resubmitted to the PMA. Once the PMA has determined the CPS is consistent with the CP, the OA can approve and sign the CPS.

A CA Operator may claim compliance of a given CPS with the relevant CP only once an independent auditor competent in the operation of a PKI has provided the CA Operator with an audit report substantiating compliance.

1.5.5 Waivers

Waivers shall not be issued. Instead, CP and/or CPS changes shall be made, or remediation activities shall be scheduled and implemented.

1.6 DEFINITIONS AND ACRONYMS

See Sections 12 and 13 of the CP.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

The OA shall operate repositories to support CA operations.

Entity PKIs are responsible for operation of repositories to support their PKI operations.

Entities who cross-certify with the CA shall ensure interoperability with the CA Repository.

Repository Obligations

CAs may use a variety of mechanisms for posting information into a Repository as required by this CP. These mechanisms at a minimum shall include:

- Repository that is accessible through HTTP
- Availability of the information as required by the Certificate information posting and retrieval stipulations of this CP and
- Access control and communication mechanisms when needed to protect Repository information as described in later sections

Optionally, an X.500 Directory Server System may also function as a Repository to complement a Web Server System.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

Publication of Certificates and Certificate Status

CA and end entity certificates shall be published to URIs that are accessible, with no access controls when accessed by relying parties.

The OA shall publish all CA Certificates issued by or to the FAA and all CRLs issued by the FAA in the FAA Repository.

All encryption Public Key Certificates issued by CAs to digital Certificate end entities shall be published to the respective applicable FAA Repositories, as set forth in the applicable CPSs.

For the FAA, mechanisms and procedures shall be designed to ensure CA Certificates and CRLs are available for retrieval 24 hours a day, 7 days a week, with a minimum of 99% availability overall per year.

Publication of CA Information

The FAA NPE-CP shall be published and publicly available on their associated website.

All encryption certificates issued by entity CAs to end entities shall be published to the respective applicable entity repositories.

All CRLs, ARLs, CA Certificates, and CA cross certificates issued by entity CAs shall be published to the respective and applicable repositories, if they are within their stated validity period.

Furthermore, all the CRLs and ARLs shall be accessible via HTTP. Interoperability

Where Certificates and CRLs are published in a X.500 Directory Server System, standards-based schemas for directory objects and attributes are required and shall be consistent with the Repository Profile.

Note: The upcoming paragraph refers to directory server attributes e.g., cross certificate pair, CA certificates, standards-based schemas or objects defined by the X.500 or X.501 standards.

Entity Repositories as defined above shall be interoperable as required with all repositories operated by CAs with which the Entity PKI is cross-certified. The following interoperability profile is defined:

- Naming: CA Certificates shall be stored in the Directory in the entry that appears in the Certificate subject name. The issuedByThisCA element of crossCertificatePair shall contain the Certificate(s) issued by a CA whose name the entry represents. CRLs shall be stored in the Directory in the entry that appears in the CRL issuer name.
- Object Class: Entries that define CAs shall be members of pkiCA cpCPS auxiliary object classes. Entries that describe end-users shall be defined by the inetOrgPerson class, which inherits from other classes: person, and organisationalPerson. These entries shall also be a member of pkiUser auxiliary object class
- Attributes: CA entries shall be populated with the cACertificate, crossCertificatePair, and CertificateRevocationList as applicable. User entries shall be populated with userCertificate attribute containing that user's Encryption Certificate.

Privacy of Information

A CA or RA shall protect the Privacy of Subscribers and Subscribers' Employers based on applicable laws. Subscribers and Subscribers' Employers shall authorize a CA or RA to collect and use personal data in accordance with section 9.4 and applicable law.

2.3 TIME OR FREQUENCY OF PUBLICATION

This CP and any subsequent changes shall be made publicly accessible within thirty (30) days of approval.

Certificates and Certificate status information shall be published as specified in Section 4.

The CA's public information identified in Section 2.2 shall be published prior to the first Certificate being issued in accordance with this CP.

2.4 ACCESS CONTROLS ON REPOSITORIES

The OA CAs shall protect any Repository information not intended for dissemination or modification.

For CAs, Certificates that contain the Universally Unique Identifier (UUID) in the subject alternative name extension shall not be distributed via publicly accessible repositories (i.e., HTTP).

Certificate Policy

See section 2.2.2

Certificates and CRL

CAs shall be the only entities authorized to create, modify, or otherwise maintain Certificates or CRLs.

The authentication and protection mechanism used for these operations shall be commensurate with the highest level of assurance issued by the CA.

The Certificate Repository including certificates and CRLs shall be protected against unauthorized modification.

Read only access to both certificates and CRLs within the certificate repository shall be granted to anonymous users (i.e. authentication type “none”) of the certificate repository.

3. IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

Types of Names

The CAs shall only generate and sign Certificates that contain a non-null subject Distinguished Name (DN). Certificates issued by the CAs may also include alternative name forms.

For Certificates issued by CAs, in accordance with RFC 5280, the following rules apply:

- All Certificates shall include a non-NULL subject DN and a non-NULL issuer DN
- The DN may be formed as either internet domain component or geo-political forms
- Certificates may include Subject Alternative Names if marked non-critical

Certificates shall indicate whether or not the Subscriber is associated with an Affiliated Organization by taking one of the following forms:

For Certificates with an Affiliated Organization	Affiliated Organization name is present in the Distinguished Name as an organization (o), organizational unit (ou), or domain component (dc) value.
For Certificates with no Affiliated Organization	“Unaffiliated” is present in the last organizational unit attribute in the Distinguished Name Entity CA name is present in the organizational unit attribute in the Distinguished Name.
For TLS Domain Validated Certificates	Organizational unit attribute shall not be present.

Need for Names to Be Meaningful

Names used in the Certificates shall identify the Person or NPE to which they are assigned in a meaningful way.

When DNs are used, the Directory information tree shall accurately reflect organizational structures.

The Common Name (CN) shall respect name space uniqueness requirements, shall not be misleading, and shall be easily understood by humans. For people, this shall typically be a legal name. For Roles, this shall be a clear representation of the role (e.g., Purchasing Agent, System Administrator, and Final Quality Assurance Engineer). For organizations or corporations possessing an organizational *Medium-Assurance* hardware code-signing Certificate, this shall be the officially recognized legal name or registration number of the organization or corporation. For equipment, this may be an IP address, fully qualified domain name, URL, model name and serial number, asset tag, or an application process. This does not preclude the use of pseudonymous Certificates as defined in Section 0.

When User Principal Names (UPN) are used, they shall be unique and accurately reflect organizational structures.

Name space shall be limited as specified in Section 7.1.5

Anonymity or Pseudonymity of Subscribers

CA Certificates issued by CAs shall not contain Anonymous or Pseudonymous identities.

DNs in End-Entity Certificates issued by CAs may contain a pseudonym (such as a large number) if name space uniqueness requirements are met, and the pseudonym is reversible.

Rules for Interpreting Various Name Forms

The PMA is responsible for controlling name space for the CA. CAs shall specify the party responsible and accountable for controlling its name space within its CP.

Rules for interpreting name forms shall be defined in Certificate profiles located within a CP directly (see Section 10) or a referenced certificate profile.

Uniqueness of Names

Distinguished Name global uniqueness shall be enforced by the FAA.

The OA is responsible for ensuring name uniqueness in Certificates issued by the CA.

The Distinguished Name of a Subscriber shall remain unique even when multiple Certificates are issued to the same Subscriber.

The CPS shall specify how name uniqueness will be ensured, including in circumstances where a Person or NPE has the same name as a Person or NPE issued a Certificate in the past. The CPSs shall also describe how names shall be allocated within the Subscriber community to guarantee name uniqueness among current and past Subscribers (i.e., if “John Q Smith” leaves a CA’s community of Subscribers, and a new, different “John Q Smith” enters the community of Subscribers, how will these two people be provided unique names) thereby guaranteeing uniqueness of names over time.

Practice Note: *Relying party applications may assume a one-to-one relationship between a Certificate and a Distinguished Name/subject alternative name. However, such applications may not be interoperable with PKIs that issue multiple Certificates to the same Subscriber thereby creating a one-to-many relationship if only the Distinguished Name and/or subject alternative names are verified by the Relying Party application.*

Recognition, Authentication, and Role of Trademarks

Subscribers shall not use names in their Certificate Applications that knowingly infringe upon the Intellectual Property Rights of others. The CA shall reserve the right to make all decisions regarding Subscriber names in all assigned Certificates. No CA operating under this CP shall be required to determine whether a Subscriber has Intellectual Property Rights in the name appearing in a DN or to arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark. A CA operating under this CP shall be entitled, without liability to any Subscriber, to reject or suspend any Certificate because of such dispute.

Name Claim Dispute Resolution

The PMA shall resolve, or cause to be resolved, any name collision related to the PKI that is brought to its attention. Furthermore, CAs shall not knowingly use trademarks in names unless the Subject has the rights to use that name, in accordance with section 9.5.3.

3.2 INITIAL IDENTITY VALIDATION

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 that corresponds to the Public Key in the Certificate Request.

Specifically for signature keys, this may be done by the subscriber using its private key to sign a value and providing that value to the CA. The CA shall then validate the signature using the party's public key. The PMA may allow other mechanisms that are at least as secure as those cited here.

In the case where a key is generated by the CA or RA either (1) directly on the party's hardware or software token; or (2) in a key generator that benignly transfers the key to the party's token, proof of possession is not required.

In the case of an aircraft avionics component that is not capable of generating its own keys (e.g., for an AMS Aircraft Certificate), this may only be possible from a separate computer before the key is transferred into the aircraft avionics component. Subsequent to proof of possession, the Private Key shall be distributed to the aircraft avionics in a manner consistent with Section 6.2.

Authentication of Organization Identity

Requests for CA issuance of Cross-Certificates shall include the Organization name, address, and some documentation of the existence of the Organization. The OA shall verify the information provided and the authenticity of the requesting representative, and the representative's authorization to act in the name of the Organization prior to issuance of any Cross-Certificate.

Requests for Subscriber Certificates with an Affiliated Organization list in the distinguished name in the organization field shall include the either:

- the Organization name, address, and some documentation of the existence of the Organization (such as articles of incorporation or corporation number).
- its Dun and Bradstreet (DUNS) identifier if doing business within the United States of America or elsewhere where this identifier is commonly used or verification with another third party (e.g., Tax authority, country, state or province corporate registry) the existence of the company with record identifier.
- A letter from its authorized representative officially requesting said Certificate; and
- A face-to-face meeting or supervised remote identity proofing as described in Section 3.2.3.1 and 3.2.3.2 with the RA or CA and an authorized representative of the Organization carrying the appropriate power of attorney.

Or

A National Authority issued digital identity to an official from the affiliated organization. e.g., PIV, CAC, EIDAS credential from the official representing the affiliated organization.

The CA or RA, as applicable, shall verify the information provided, the authenticity of the requesting representative, and the representative's authorization to act in the name of the Organization prior to issuance of end user Certificates. Requests for end user Certificates other than unaffiliated Subscribers shall include the name of the Organization and shall be verified with the identified Affiliated Organization.

Authentication of Individual Identity

Successful authentication shall bind together the process documentation, Public Key, Applicant identity information, and Applicant.

3.2.1.1 NPE Subjects

NPEs, including Computing and communications Devices (routers, Firewalls, Servers, etc.), may be named as Certificate Subjects. In such cases, the NPEs shall have a human sponsor, known as a Device Sponsor. The Device Sponsor applying for a Certificate for an NPE shall hold an individual Certificate of assurance equal to or greater than that of the Certificate being requested. This can either be a Certificate from the Device Sponsor's FAA PIV card or a Certificate issued by the same CA from which the current Certificate is being requested.

The sponsor is responsible for providing the following registration information for NPEs that are devices:

- Equipment identification (e.g., serial number, asset tag, aircraft registration number, aircraft part number) or service name (e.g., Domain Name Service (DNS), Fully Qualified Domain Name, IP address, ACARS Message Security (AMS) subscriber identifier per Section 7.1.4, or other network address) sufficient to uniquely identify the Subject
- Equipment Public Keys
- Equipment authorizations and attributes (if any are to be included in the Certificate)
- Contact information to enable the CA or RA to communicate with the sponsor.
- When required aircraft, aircraft components, and aircraft on-board systems may be named as Certificate Subjects. In such cases, all of the requirements above apply, and the sponsor shall also provide relevant Aircraft National Registration Paperwork. In the case a human sponsor is changed, the new sponsor shall review the status of each NPE under his/her sponsorship to ensure it is still authorized to receive Certificates.

The CPS shall describe procedures to ensure that all certificate accountability is maintained.

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 sponsor (using Certificates of equivalent or greater assurance than that being requested).
- In person or Supervised Remote Registration by the sponsor, with the identity of the sponsor confirmed in accordance with the requirements of Section 2.

Supervised Remote Identity Proofing shall meet the criteria specified in NIST SP 800-63A [2] Section 5.3.3.

All Device Sponsors (including when Device Sponsor is changed) shall be accountable for all NPE Certificates under their sponsorship to ensure the NPEs are authorized to be issued Certificates or to continue to possess Certificates issued by the CA.

[2] https://pages.nist.gov/800-63-3-Implementation-Resources/63A/srip/)

3.2.1.2 Individual Subjects

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.

For low-assurance Certificates, an in-person appearance is not required, but corporate affiliation of the Applicant shall be provably established, preferably by another Subscriber from that company who did personally appear. For other Assurance Levels, identity shall be established by in-person proofing before the RA, Trusted Agent, or a person certified by a state or government as being authorized to confirm identities; information provided shall be verified to ensure legitimacy. A trust relationship between the Trusted Agent and the Applicant that is based on an antecedent may suffice as meeting the in-person identity proofing requirement.

The process documentation and authentication requirements shall include the following:

Personally Identifiable Information (PII) may be collected and stored to the extent permitted by applicable law (see section 9.4). CAs and RAs are responsible for ensuring that they comply with all applicable laws (see section 9.4) when collecting such information.

- The identity of the Person performing the identity verification,
- A signed declaration by that Person that he or she verified the identity of the Applicant as required by the applicable CP which may be met by establishing how the Applicant is known to the verifier as required by this CP,
- The date and time of the verification.

For *Low* Assurance Levels, the following information shall be recorded (through in person or via a secure remote session):

- the full name, including surname and given name(s) of the Applicant,
- the full name and legal status of the Applicant's Employer,
- a physical address or other suitable method of contact (which may be an email address),
- an acknowledgement signed by the Applicant indicating their acceptance of the Privacy Policy.

For *Medium Assurance* Levels, The TA may confirm address of record by validating information supplied by the applicant that is not contained on any supplied piece of identity evidence. Self-asserted address data that has not been confirmed in records shall not be used for confirmation.

For *Medium* Assurance Levels, the Applicant shall provide, through in-person or secure remote session, all the requirements for low-assurance, and in addition:

- provide date and place of birth or other attribute(s) which may be used to uniquely identify the Applicant,
- present one valid national government-issued photo ID, or two valid non-national government IDs, one of which shall be a recent photo ID (e.g., driver's license, passport),
- have recorded with the above information for all Assurance Levels, 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.

3.2.1.3 Individual Subject for Role Certificates

Subscribers may be issued Role Certificates. In addition to the stipulations below, authentication of individuals for Role Certificates shall follow the stipulations of Section 3.2.3.2 of this CP. A Role Certificate shall identify a specific role on behalf of which the Subscriber is authorized to act rather than the Subscriber's name. A role Certificate may be used in situations where Non-Repudiation is desired. Role based Certificates shall not be a substitute for an individual Subscriber Certificate. Multiple Subscribers can be assigned to a role at the same time; however, the signature or identity Key Pair shall be unique to each Role Certificate issued to each individual. The Encryption Key Pair and Encryption Certificate may be shared by the individuals assigned the role.

Subscribers issued Role Certificates shall protect the corresponding role credentials in the same manner as individual credentials.

The procedures for issuing Role Certificates shall comply with all other stipulations of this CP. For role Signature and Identity Certificates, the individual assigned the role, or the role sponsor may act on behalf of the Certificate Subject for Certificate management activities such as issuance, rekey and Revocation. For role Encryption Certificates, only the role sponsor may request issuance, rekey and revocation.

The CA or the RA shall record the information identified in Section 3.2.3 for a Sponsor Organization associated with the Role Sponsor before issuing a Role Certificate. The sponsor shall hold an individual Certificate in his/her own name at the same or Higher Assurance Level as the Role Certificate. The CA or the RA shall validate with the role sponsor that prospective individual Subscribers have been approved for Role Certificates.

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

3.2.1.4 Individual Subject for *TSP Mediated Signature* Certificate

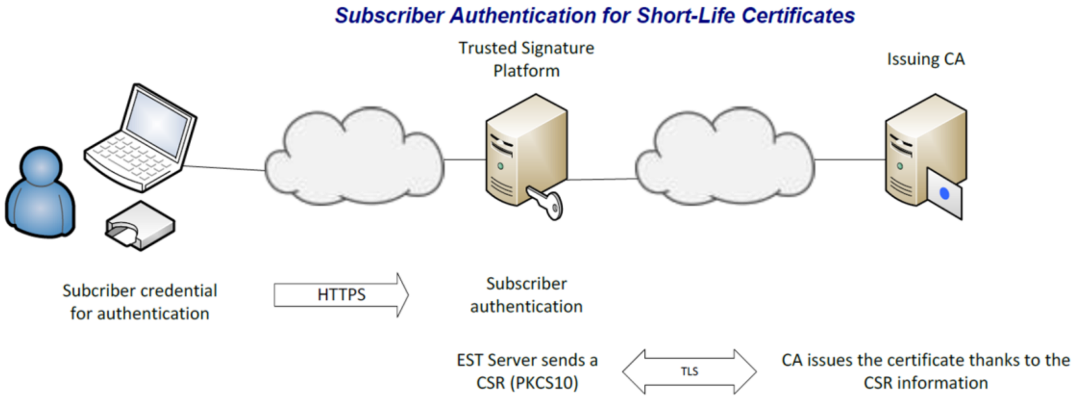
Subscribers may be issued *TSP Mediated Signature* Certificates. A TSP *Mediated Signature* Certificate shall identify the Subscriber using the Authentication service of the Signature Trust Platform (STP). A *TSP Mediated Signature* Certificate may be used in situations where Non-Repudiation is desired for the unique purpose of signature. Authentication of the Subscriber shall be carried out in accordance with Section 3.2.3.2 based upon the type of Certificate issued.

The Trusted Platform issuing the Certificate Signing Request (CSR) for *TSP Mediated Signature* Certificates, ensuring the e-signature creation, verification, rekey, renewal, revocation and logging all the transactions (who signed what and when) shall protect all the functions pertaining to the e-signature and all the assets supporting those functions with a level commensurate with the level of assurance of the issued Certificates.

The Enrollment over Secure Transport(EST) is a cryptographic protocol that describes an X. 509 certificate management protocol targeting public key infrastructure (PKI) clients that need to acquire client certificates and associated certificate authority (CA) certificates. EST is described in RFC 7030 and ACME RFC 8555. EST profiles Certificate enrollment for Clients using Certificate Management over Cryptographic Message Syntax (CMC) over a secure transport. According to the IETF, EST "describes a simple, yet functional, Certificate management protocol targeting Public

Key Infrastructure (PKI) Clients that need to acquire Client Certificates and associated Certification Authority (CA) Certificates”.

EST uses Public-Key Cryptography Standards (PKCS#10) and IETF Cryptographic Message Syntax for Certificate Requests and Certificate definitions, respectively. It uses Transport Security Layer (TLS) for the secure transport of messages and Certificates. In EST, the Certificate Signing Request (CSR) can be tied to a requestor that is already trusted and authenticated with TLS. EST provides cryptographic agility. It supports elliptic curve cryptography (ECC).


Subscriber Authentication for Short-Life Certificates
Trusted Signature Platform
Issuing CA
Subcriber credential for authentication
HTTPS
Subscriber authentication
EST Server sends a CSR (PKCS10)
TLS
CA issues the certificate thanks to the CSR information

The credential used for Subscriber’s authentication shall be at the same or higher level of assurance than the *TSP Mediated Signature* Certificate issued for signature (e.g., A Subscriber using a “low” level of assurance Certificate to authenticate should be issued a “*TSP Mediated Signature Low*” level of assurance Certificate and shall not be issued a “*TSP Mediated Signature Medium*” level of assurance Certificate.)

3.2.1.5 Human Subject Identity Proofing via Antecedent Relationship

The following requirements shall apply when human Subscriber identity is verified using antecedent relationship with the Sponsoring Organization:

1) The Applicant does not personally need to appear before a verifier (usually a Trusted Agent) but shall use a digital proof of possession process, at the same or higher level of assurance as the requested certificate, using one of the items below.

2) The Applicant and the TA or RA shall have an established working relationship with the Sponsoring Organization. An example of “established working relationship” is the Person is employed by the Sponsoring Organization. Another example of “established working relationship” is the Person is consultant to the Sponsoring Organization or is employed by a contractor of the Sponsoring Organization. The relationship shall be sufficient to enable the TA or RA to, with a High degree of certainty, verify that the Applicant is the same Person that was identity proofed. An example to meet this requirement is when the Applicant and TAs or RAs are employed by the same company and the company badge forms the basis for the Applicant authentication.

3) The Applicant shall present a valid Sponsoring Organization-issued photo ID. This photo ID shall have been issued on the basis of previously performed in-person identity proofing using one valid National Government-issued Picture ID, or two valid non-National Government IDs, one of which shall be a recent photo ID (e.g., Driver’s License, Passport).

4) The TA or RA shall record the following:

    a. His/her own identity.

   b. Unique identifying number from the Identifier (ID) of the verifier.
   c. Unique identifying number from the Applicant’s Sponsoring Organization-issued photo ID.
   d. Date and time of the identity verification; and
   e. Date and time of Sponsoring Organization-issued photo ID, if applicable.

5) The verifier shall sign a declaration that he or she verified the identity of the Applicant as required by the applicable Certificate Policy which may be met by establishing how the Applicant is known to the verifier as required by this Certificate Policy; and
6) The Applicant shall sign a declaration of identity using a handwritten signature or appropriate Digital Signature.

3.2.1.6 Human Subject Re-Proofing following loss, damage, or Key Compromise

If human Subscriber credentials containing the private keys associated with the Public Key Certificates are lost, damaged, or stolen, the Subscriber may be issued new Certificates according to the re-proofing provisions in this Section.

The re-proofing provisions are the same as those followed for the initial identity proofing Section 3.2.1.1 or Section 3.2.3.2 with the following modifications:

- The validity period of the Certificates issued using this process shall not exceed the identity-reproofing requirements in Section 0.
- Only one National Government-Issued Photo ID or non-National Government issued Photo ID (e.g., Driver’s License, Passport) is required.

Practice Note: *As Biometric authentication accuracy degrades with the time elapsed since initial collection, Entity PKIs may desire to update Biometric(s) after a match has been made.*

Non-verified Subscriber Information

Information that is not verified shall not be included in Certificates.

Validation of Authority

Prior to issuing Cross-Certificates, the Issuing CA shall validate the external PKI domain CA Certificate requestor’s authorization to act in the name of the external PKI domain CA. In addition, the CA shall obtain PMA approval prior to issuing CA Certificates.

Certificates that contain explicit or implicit organizational affiliation shall be issued only after ascertaining the Applicant has the authorization to act on behalf of the organization in the asserted capacity.

To obtain a medium-assurance Certificate, any prospective Subscriber whose employer is not the Issuing CA shall present at the time of authentication a letter from their employer authorizing him or her to obtain a Certificate of this type, if there has not been a previous request signed (digitally or otherwise) by an authorized representative of the employer. For a low-assurance Certificate, the same may be required for an Applicant who did not appear in person before the RA, as per Section 3.2.3.

- For Certificates to be loaded in aircraft avionics, a document proving the Applicant's employer's status as an airline or as another type of legitimate operator of the given aircraft, such as a copy of aircraft registration documents shall be provided.
- For Certificates used by ground entities that communicate with aircraft avionics, a document proving the Applicant's employer's status as an airline as above, or as a supplier of datalink service to an airline, such as a signed contract to that effect, shall be provided.
- For all code-signing Certificates, a document shall be provided proving the Subscriber's right to create and publish software within the community.
- To obtain a TSP Mediated Signature Medium-Assurance Certificate, any prospective Subscriber shall, at a minimum, be authenticated based on a Medium-Assurance Certificate obtained as described here above.
- To obtain a TSP Mediated Signature Low-Assurance Certificate, any prospective Subscriber shall, at a minimum, be authenticated based on a Low-Assurance Certificate obtained as described here above or a Non-PKI credential such as out of band token or onetime password (OTP) token.

Criteria for Interoperation

The PMA shall determine the criteria for cross-certification with the CA and shall approve a cross-certification criteria and methodology. Such methodology shall include the following verifications:

- CP-to-CP mapping has completed and found the CPs to be equivalent
- PKI has successfully passed a Compliance Audit (see Section 8 of this CP)
- Verification that Certificate Profiles and Certificates are compliant with the applicable CP
- Verification that Certificate Status (e.g., CRL, OCSP) are compliant with the applicable CP
- Verification that CA Certificates and Certificate Status information are published and available for Relying Parties

Interoperating CAs shall adhere to the following requirements:

- Complete Policy mapping with the CA CP with results satisfactory to both parties;
- Operate a CA that has undergone a successful Compliance Audit pursuant to Section 8 of this CP and as set forth in the Subject CA's CP;
- Issue Certificates compliant with the profiles described in this CP, and make Certificate status information available in compliance with this CP;
- Assert the Certificate Policy OIDs as outlined in Section 1.2.2; and
- Publish CA Certificate and Certificate status information.

It shall be the responsibility of the participating entity PMA to ensure that these requirements are met prior to the entity PMA authorizing interoperation agreement.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

Identification and Authentication for Routine Re-key

For Re-key of a Bridge or Subordinate CA, the CA shall be authenticated through use of a Private Key and corresponding valid Certificate or one of the initial identity proofing processes described in Section 3.2.1.1 and Section 3.2.3.2 for the CA's trusted individual. If it has been more than three years since a CA was identified, identity shall be re-established through the initial identity proofing process as required in Section 3.2.

Subscribers shall be authenticated using the current signature key or one of the initial identity proofing processes described in Section 3.2.1.1 and Section 3.2.3.2. For *Medium* assurance and above, if it has been more than nine years since the Subscriber was identified as required in Section 3.2, identity shall be re-established through the initial identity proofing process. For *Low* assurance Certificates, there is no further requirement for the frequency of the identity proofing process.

All requests for Re-key shall be authenticated by the CA, and the subsequent response shall be authenticated by the Subscriber. This may be done by an on-line method in accordance with RFC 4210, or other suitable equivalent method as determined by the PMA.

When current private key and corresponding valid Certificate is used for identification and authentication purposes, the life of the new Certificate shall not exceed the initial identity-proofing times specified in the paragraphs 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.

Identification and Authentication for Re-key after Revocation

After a Certificate has been revoked, other than during a renewal, Update, or to replace a lost/stolen/damaged credential, the Subscriber is required to go through the initial Registration processes described in Section 0 to obtain a new Certificate unless the Subscriber can be authenticated with a non-revoked Certificate of equal or Higher assurance issued from the same CA.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

The CA or RA shall authenticate a request for Revocation of a Certificate. The CA or RA may authenticate requests to Revoke a Certificate using that Certificate's Public Key, regardless of whether the associated Private Key has been compromised.

Other Revocation request authentication mechanisms may be used as well, such as challenge-response questions combined with a completed standard CA Revocation Request form that was sent to the Certificate holder at the time of the revocation request.

All Revocation requests shall be logged. See Section 4.9 for additional stipulations.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

The CA, RA, TA, other parties confirming identities and subscribers shall manage certificates and corresponding public and private keys safely at their initial creation through their full life cycle. Communication amongst the parties shall have security measures (e.g., source authentication, integrity, non-repudiation, or confidentiality) applied to them commensurate with the LOA of the certificate being managed. When cryptography is used, the mechanism shall be at least as strong as the certificates being managed. For example, a web site secured using TLS certificates issued under medium-software policy and set up with appropriate algorithms and key sizes shall satisfy integrity and confidentiality requirements for medium-software certificate management.

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

4.1 CERTIFICATE APPLICATION

This section specifies requirements for initial application for Certificate issuance.

The PMA shall establish and publish its criteria and procedures describing how other external CAs may cross-certify, how CAs may subordinate, and how Subscribers may apply for Certificate(s).

Submission of Certificate Application

For FAA Line of Business (LOB) CAs, their CP shall define submission processes for CAs and Subscribers consistent with the subsections below.

4.1.1.1 Application for Organizational Certificates

An RA, acting on behalf of the Subscriber shall submit a Certificate application to the CA.

4.1.1.2 Application for Subscriber Certificates by an individual

The Subscriber or RA, acting on behalf of the Subscriber shall submit a Certificate application to the CA.

4.1.1.3 Application for Subscriber Certificates on behalf of an NPE

The Device Sponsor, who needs to be a Subscriber or an RA acting on behalf of the Subscriber, shall submit a Certificate application to the CA.

4.1.1.4 Application for *TSP Mediated Signature* Certificates by a Subscriber

The RA hosted in the STP acting on behalf of the Subscriber shall submit a Certificate application in an EST format to the CA after successful authentication of the Subscriber by the trusted authentication service of the Signature Trust Platform.

4.1.1.5 Application for CA Certificates

For CA Certificate applications to the Root, Principal or Subordinate CA, an authorized representative of the Subject CA shall submit the application to the PMA.

Enrollment Process and Responsibilities

Entity CAs applying for cross-certification are responsible for providing accurate information in their Certificate applications. Upon issuance the OA shall manually check the Certificate to ensure each field and extension is properly populated with the correct information before the Certificate is delivered to the Subscriber.

Entity CA CP shall describe the enrollment process and responsibilities for its cross-certified and Subordinate CAs and Subscribers.

All communications among PKI authorities materially supporting the Certificate application and issuance process shall be authenticated and protected from modification.

Applicants for Public Key Certificates shall be responsible for providing accurate information in their applications for certification.

Information regarding attributes shall be verified via those bodies that have authority to assign the information or attribute. Relationships with these offices or roles shall be established prior to commencement of CA duties and shall be described in the applicable CPS.

For CA Certificates, the PMA shall verify all authorizations and other attribute information received from an Applicant CA.

All Subscribers shall agree to be bound by a relevant Subscriber Agreement.

4.1.1.6 Subscriber Certificates

The Applicant and the RA shall perform the following steps when an Applicant applies for a Certificate:

- establish and record identity of Subscriber.
- obtain a Public/Private Key Pair for each Certificate required.
- establish that the Public Key forms a functioning Key Pair with the Private Key held by the Subscriber.
- provide a point of contact for verification of any roles or authorizations requested; and
- verify the authority of the Applicant.

These steps may be performed in any order that is convenient for the RA and Subscribers, and that do not defeat security; but all shall be completed prior to Certificate issuance. Any electronic transmission of shared secrets shall be protected (e.g., encrypted, or using a split secret scheme where the parts of the shared secret are sent using multiple, separate channels) using means commensurate with the requirements of the data to be protected by the Certificates being issued.

4.1.1.7 CA Certificates

The PMA shall make the procedures and application form available to FAA LOBs requesting issuance of a CA Certificate from an FAA Root or Subordinate CA.

The Root CA shall certify Principal and Subordinate CAs implementing this CP only as authorized by the PMA. A CPS written to the format of the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework [RFC 3647], shall accompany the applications of the requesting Sub CA. The CPS shall conform to the CP.

Requests by external PKI domain CAs for CA Certificates from an CA shall be submitted to the PMA using the contact provided in Section 1.5 of the CP.

The PMA shall evaluate the submitted application in accordance with procedures that it shall develop, publish, and make a determination regarding whether to issue the requested Certificate(s), and what policy mapping to express in the Certificate(s), if applicable.

The PMA shall commission a CP/CPS compliance analysis prior to authorizing the Operational Authority (OA) to issue and manage CA Certificates operating within the PKI Domain.

Entity CAs shall only issue Certificates asserting the OIDs outlined in the CA CP upon receipt of written authorization from the PMA, and then may only do so within the constraints imposed by the PMA or its designated representatives.

4.2 CERTIFICATE APPLICATION PROCESSING

Information in Certificate applications shall be verified as accurate before Certificates are issued.

It shall be the responsibility of the RA, or, in the case of a CA Certificate, the PMA, to verify that the information in a Certificate Application is accurate.

The applicable CPS shall specify procedures to verify information in Certificate applications.

Performing Identification and Authentication Functions

For the CA, the identification and authentication of the Applicant shall be performed by the OA.

For entity CAs, the identification and authentication of their subscribers shall meet the requirements specified in their associated CPs. The entity CA CP shall identify the components of the entity PKI (e.g., CA, RA or TA) that are responsible for authenticating the subscriber’s identity in each case.

Before the issuance process completes, a Subscriber shall be required to sign a Subscriber Agreement, which includes the Subscriber’s obligation to protect the Private Key and only use the Certificate and Private Key for authorized purposes. See section 4.5.1, 4.5.3, and 9.6.3.

For *TSP Mediated Signature* Certificates, the Subscriber Private Key protection is the responsibility of the Signature Trust Platform.

The Issuing CAs shall check for Certification Authority Authorization (CAA) records on FQDNs. If CAA records are present, the Issuing CAs shall follow the processing instructions on the property tags for each DNS Name in the SAN extensions of the to-be-issued Certificates as defined in RFC 8659. Furthermore, the Issuing CAs shall define the practices for processing CAA records in the CPS.

Approval or Rejection of Certificate Applications

For the CA, the PMA may approve or reject a Certificate application (see Section 1.3.1.1).

For CAs, the applicable CPS shall define the organization that may accept or reject a certificate application.

The CA or RA shall approve a Certificate application if all of the following conditions are met:

- successful identification and authentication of all required Subscriber information; and
- funding (if applicable) is available.

The CA or RA shall reject a Certificate application if any one or more of the following conditions arises:

- identification and authentication of all required Subscriber information cannot be completed.
- the Subscriber fails to furnish supporting documentation upon request.
- the Subscriber fails to respond to notices within a specified time.

- payment (if applicable) has not been received; or
- the RA or CA believe that issuing a Certificate to the Subscriber may bring the CA into disrepute.

Time to Process Certificate Applications

Individual Identity shall be confirmed no more than 90 days before initial Certificate issuance.

Practice Note*: Individual identity should be confirmed no more than 30 days before initial Certificate issuance unless there are extenuating circumstances.*

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 the applicable CP and corresponding CPS.

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

The issuance of an unauthorized certificate from any CA shall be detected within 30 minutes.

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 trusted to confirm Subscriber information, then these internal databases shall be protected from unauthorized modification to a level commensurate with the level of assurance of the Certificate being sought.

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

When information is obtained through one or more data sources, the OA shall ensure there is an auditable chain of custody.

CA Actions during Certificate Issuance

A Certificate is created and issued following the approval of a Certificate Application by a CA or following receipt of an RA's request to issue the Certificate. The CA creates and issues to a Certificate Applicant a Certificate based on the information in a Certificate Application following the CA approval of such Certificate Application. The CA shall authenticate 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 the CA shall publish the Certificate to a Repository in accordance with the CA CP and the applicable CPS. This shall be done in a timely manner.

Notification to Subscriber of Certificate Issuance

CAs (or RA) shall notify the Applicant (CA or Subscriber) of Certificate issuance and provide Subscribers with access to the Certificates by notifying them that their Certificates are available and the methods for obtaining them. Such methods shall be described in the appropriate CPS.

The OA shall inform the PMA of any Certificate issuance to a CA by a Root or Intermediate CA. The PMA shall inform the authorized instance of such Applicant CA of the successful Certificate issuance.

4.4 CERTIFICATE ACCEPTANCE

Before a Subscriber can make effective use of its Private Key, a PKI Authority shall convey to the Subscriber its responsibilities as defined in Sections 4.5.1, 4.5.3., and 9.6.3.

Conduct Constituting Certificate Acceptance

A Subscriber shall explicitly indicate acceptance or rejection of the Certificates to the CA as set forth in the respective CPS.

For the issuance of CA Certificates to Subordinate CAs, the PMA shall set up an acceptance procedure indicating and documenting the acceptance of the issued CA Certificate.

For *TSP Mediated Signature* Certificates, the Subscriber acceptance is tacitly performed through the signature acceptance process.

Publication of the Certificate by the CA

As specified in Section 0, all CA Certificates shall be published in Repositories.

Certificates shall be published according to Section 2 as soon as they are issued.

There is no need of publication for *TSP Mediated Signature* Certificates.

Notification of Certificate Issuance by the CA to other entities

As shall notify the PMA and all Entities cross-certified with the FAA of all CA Certificate issuances as detailed in the applicable CPS.

For Entity CAs, the PMA shall be notified at least two weeks and a day prior to the issuance of a new CA Certificate or issuance of CA Certificates external to the Entity's PKI domain. The notice period shall commence upon written acknowledgement of the OA. In addition, all new artifacts (CA Certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the CA Certificate issuance shall be provided to the PMA within 24 hours following issuance.

4.5 KEY PAIR AND CERTIFICATE USAGE

Subscriber Private Key and Certificate Usage

Subscribers shall protect their Private Keys from access by other parties.

Subscribers and CAs shall use their Private Key as specified through Certificate Extensions, including the key usage, extended key usage extensions, and Certificate policies in the associated Certificate.

Use of the Private Key corresponding to the Public Key in the Certificate, aside from initial proof-of-possession transaction with the CA, shall only be permitted once the Subscriber has agreed to the Subscriber Agreement and accepted the Certificate (See section 9.6.3). The Certificate shall be used lawfully (See Section 9.6.3) in accordance with the Subscriber Agreement and the terms of this CP.

Subscribers and CAs shall discontinue use of the Private Key upon expiration or Revocation of the Certificate.

TSP Mediated Signature Certificates and associated Private Keys are limited to the remote signature purpose using the signature service provided by the Signature Trust Platform.

Relying Party Public Key and Certificate Usage

Relying parties shall accept Public Key Certificates and associated Public Keys for the purposes intended as constrained by the extensions (such as key usage, extended key usage, Certificate policies, etc.) in the Certificates. It is the Relying Party's responsibility to determine the appropriateness of the use of a Certificate for any given purpose and determine that the Certificate shall, in fact, be used for an appropriate purpose that is not prohibited or otherwise restricted. It is also the Relying Party's responsibility to check the status of a Certificate before reliance on that Certificate and verify any signatures upon which they rely.

In circumstances where a Time Stamping service is used, applications verifying software packages signed with an organizational *Medium* assurance code-signing Certificate, or role-based code-signing Certificate used for Aircraft Software Signature, shall check the timestamp, and shall reject any software package which either does not have a timestamp issued by a recognized Time Stamp Authority, or whose timestamp shows a time later than the time of the check, or whose timestamp shows a time before the 'Valid before' date of the Certificate signing the software package.

For *TSP Mediated Signature* Certificates, the RA hosted in the STP creates a proof file for each Certificate issuance and signature creation. This proof file contains at least the signatory DN, signature date, signed data set and proof of signature validation performed by the validation service of the Signature Trust Platform.

The proof file is available following the authentication policy for signature verification on the Signature Trust Platform.

Device Sponsor Private Key and Certificate Usage

Use of the Private Key corresponding to the Public Key in the Certificate shall only be permitted once the Device Sponsor has agreed to the Subscriber Agreement and accepted the Certificate (See Section 9.6.3). The Certificate shall be used lawfully (See Section 9.6.3) in accordance with the Subscriber Agreement and the terms of this CP. Certificate use shall be consistent with the keyUsage and extendedKeyUsage extensions, in the associated Certificate.

Device Sponsors shall protect their Private Keys from unauthorized use and shall discontinue use of the Private Key following expiration or Revocation of the Certificate.

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 with a new, extended validity period and a new serial number. Certificates may be Renewed in order to reduce the size of CRLs.

After Certificate renewal, the old Certificate may or may not be revoked.

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.

Certificate renewal is not supported for *TSP Mediated Signature* Certificates.

Practice Note: *Revocation of the current certificate should only occur after the renewed certificate is in use.*

Circumstance for Certificate Renewal

A Certificate may be Renewed if the Private Key has not reached the end of its validity period, has not been revoked or compromised, and the Subscriber name and attributes are unchanged.

Certificate renewal procedures shall only be allowed for replacing OCSP Responder Certificates, SCVP Responder Certificates, Cross-Certificates, and other Device Certificates where the Certificate lifetime is purposely shorter than the Private Key lifetime.

Certificates may also be Renewed when the CA that issued the Certificates is re-keyed.

The validity period of the Certificate and Private Key shall meet the requirements specified in Section 5.6

Who may request Renewal

The OA may request renewal of a Cross-Certificate.

For CAs that support renewal, such requests shall only be accepted from the following parties:

- Device Sponsors – for NPE Certificate(s)
- Subscribers – for Human Subscriber Certificate(s)
- A device sponsor or representative of the OA may request renewal of an OCSP certificate.

Processing Certificate Renewal Requests

For the CA, Certificate renewal for reasons other than Re-key of the CA shall be approved by the OA. The PMA shall also approve and require an active Agreement (See section 1.3.1.1), which does not expire prior to the new period of the Renewed Certificate.

Certificate Renewal Requests shall be processed according to the requirements in Section 0. For renewal, however, the keys shall not change.

Notification of new Certificate issuance to Subscriber

See Section 0.

Conduct constituting acceptance of a Renewal Certificate

See Section 0.

Publication of the Renewal Certificate by the CA

See Section 0.

Notification of Certificate Issuance by the CA to other entities

See Section 0.

4.7 CERTIFICATE RE-KEY

The longer and more often a key is used, the more susceptible it is to loss or discovery. Re-keying a Certificate consists of creating new Certificates with a new and different Private Key (and serial number) and corresponding new and different Public Key, while retaining the remaining contents of the old Certificate that describes the Subject. The new Certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key. Re-key of a Certificate does not require a change to the subject Distinguished Name or subject Alternative Name(s) and does not violate the requirement for name uniqueness.

It is important that Subscribers consider periodically obtaining new keys and reestablishing identity.

A valid old certificate should be revoked as soon as the new certificate is in service. Hence, the rekeying itself shall not lead to revocation without further revocation circumstances.

Practice Note: *To ensure a smooth transition from an old Certificate to a renewed Certificate, a device certificate may need to continue using the old Certificate for an appropriately short period of time after rekeying. The duration of the short period is determined by the implementing organization.*

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.

CAs and RAs may initiate Re-key of a Subscriber's Certificates without a corresponding request from the Subscriber or Sponsor.

Who may request certification of a new Public Key

The OA may request certification of a new public key if there is sufficient rationale that the certificate is not secure.

A PMA may request re-key of its cross-certificate.

For CAs that support re-key, such requests shall only be accepted as follows:

- A Device Sponsor for its NPE Certificate(s)
- Subscribers – for Human Subscriber Certificate(s)

Processing Certificate Re-keying requests

CAs shall perform the identity proofing processes defined in Section 0 before performing re-key. Alternatively, the Certificate could be automatically re-keyed by the CA based on an electronically authenticated request from the Subscriber as per Section 3.3.1.

For the CA, the OA shall also verify the validity period associated with the new Certificate shall not extend beyond the term of the applicable agreement (See section 1.3.1.1).

For Role Signature and Role Identity Certificates, Re-key shall require the approval of the Role Sponsor if the validity period is extended beyond that already approved by the Role Sponsor.

For *Low* Assurance Certificates, the Subscriber shall be re-authenticated no less often than every second renewal or re-keying.

Notification of new Certificate issuance to Subscriber

See Section 0.

Conduct constituting acceptance of a re-keyed Certificate

See Section 0.

Publication of the re-keyed Certificate by the CA

See Section 0.

Notification of Certificate issuance by the CA to other Entities

See Section 0.

4.8 CERTIFICATE MODIFICATION

Certificate Modification consists of creating new Certificates with subject information i.e., a name or email address that differs from the old Certificate. For example, a CA may perform Certificate Modification for a Subscriber whose characteristics have changed (e.g., has just received a medical degree). The new Certificate may have the same or different subject Public Key.

If an individual's name changes (i.e., due to marriage), then proof of the name change shall be provided to the RA or the Trusted Agent in order for an Updated Certificate having the new name to be issued.

After Certificate Modification, the old Certificate may or may not be revoked, but shall not be further re-keyed, Renewed, or modified.

Certificate Modification is only supported by this CP for CA Certificates. All other requests for Certificate modification shall be treated as new Certificate applications

Circumstance for Certificate Modification

CAs may perform a Certificate Modification process in support of cases where one or more of the Subject's names or information has changed. Such circumstances include, but are not limited to, name change from marriage, post nominal change, and email address change.

Subject shall be entitled to continue with its existing Certificate before Certificate Modification is performed.

Who may request Certificate Modification

For the FAA, the OA or the Entity CA may request Certificate Modification for currently cross-certified Entity CAs.

For Entity CAs that support Certificate Modification, such requests shall only be accepted as follows:

- A PMA for its CA Certificate(s)
- A human Subject for its Certificate(s)
- A Device Sponsor for its NPE Certificate(s)

- A role sponsor for its Role Certificate(s)

Processing Certificate Modification Requests

For the CA, the validity period associated with the new Certificate shall not extend beyond the term of the original certificate.

CAs shall perform the identity proofing processes defined in Section 0 before performing re-key. However, evidence of the change to subject information shall be collected and verified as per Section 3.2 in all cases using one of the following processes:

- Initial Registration process; or
- Identification and Authentication for Re-key

In addition, the validation of the changed subject information shall be in accordance with the initial identity-proofing process.

Notification of new Certificate issuance to Subscriber

See Section 0.

Conduct constituting acceptance of modified Certificate

See Section 0.

Publication of the modified Certificate by the CA

See Section 0.

Notification of Certificate issuance by the CA to other Entities

See Section 0.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

Revocation requests shall 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. For emergency revocation, CAs shall follow the notification procedures in Section 5.7. The notice period shall begin to run upon written acknowledgement by the entity CA PMA.

OA Circumstances for Revocation

For CAs, 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.

The circumstances under which Certificates issued by the CAs shall be revoked include:

- When the PMA requests an CA-issued Certificate be revoked. This shall be the normal mechanism for Revocation in cases where the PMA determines that an PKI does not meet the Policy requirements or the requirements of the applicable Agreement (See section 1.3.1.1).
- When the OA receives an authenticated request from a designated official of the CA. CA may request Revocation for convenience. The CA shall request Revocation if it cannot

meet its obligations within this CP or the obligations corresponding to any "pass-through" policy OIDs asserted in its Cross-Certificate.

- When the CA Operational personnel determine that an emergency has occurred that may impact the integrity of the Certificates issued by the CA (e.g., Key Compromise, severe violation threatening to cross-certified parties). Under such circumstances, the following individuals may authorize immediate Certificate Revocation: Operational Authority Administrator or other personnel as designated by the Operational Authority Administrator.

The PMA shall meet as soon as practicable to review an emergency Revocation.

The circumstances under which Certificates issued by the CAs shall be revoked include:

- The Subject or authorized party requests Revocation.
- The affiliation with an Organization asserted in the DN is no longer valid. CAs shall ensure in their agreements with Subscriber Organizations that the Organization be required to notify the CA of any changes to the Subscriber affiliation.
- The affiliation with an Organization can no longer be confirmed (e.g., Organization terminates relationship with CA).
- Content in a Certificate is no longer valid (e.g., name, role, or privilege change).
- Subject can be shown to have violated the stipulations of its respective Subscriber Agreement, or this CP.
- Private Key is compromised or suspected of Compromise.

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.

Alternatively, Revocation shall occur by decision of the CA when reasonable and credible evidence exists to establish at least one of the following:

- the Certificate has been delivered based upon wrong or falsified information
- the identifying information or affiliation components of any names in the Certificate become invalid.
- the Confidentiality of a Private Key is no longer ensured or has been compromised
- the media holding the Private Key is suspected or known to have been compromised
- the Certificate fees have not been paid according to the payment terms as indicated in the relevant agreement
- the Subscriber can be shown to have violated any agreement that they may have with the CA
- the Subscriber can be shown to have violated one or more sections of this CP
- the Subscriber or the Subscriber's Employer wishes to terminate their Subscription to the CA or
- the Subscriber abandons the signature process after issuance of the *TSP Mediated Signature* Certificate before full completion of signature creation

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.

Who Can Request Revocation

A CA Certificate may be revoked upon direction of the PMA.

CAs shall accept Revocation requests from subscribers as followed:

- From Subject for its Certificates
- From Device Sponsor for its NPE Certificates
- From Role Sponsor or individual identified in the Certificate for Role Certificates
- From designated officials of Affiliated Organizations for Certificates limited to those asserting an affiliation with their organization.

CAs may permit requests from other parties (e.g., supervisors, Human Resources (HR), operational personnel).

For an organizational *Medium* assurance code-signing Certificate issued to a Corporation or other Organization as a whole, an authorized representative of the Subject Organization carrying the appropriate power of attorney, the Issuing CA or RA may request Revocation.

The CA are permitted to revoke the Certificates they issue at the issuer's sole discretion.

The RA, in case of incomplete signature creation, shall perform *TSP Mediated Signature* Certificate Revocation automatically.

Procedure for Revocation Request

A Revocation request 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). Upon receipt, the Revocation request shall be authenticated, and the corresponding Certificate shall be revoked.

For the CA, the OA Administrator shall authenticate the request and seek approval to revoke from the OA. PMA approval is not necessary under emergency circumstances as defined in Section 0.

For the CA:

- If a Subscriber leaves an Organization and the Hardware Tokens cannot be retrieved, then all Subscriber Certificates associated with that Token shall be revoked immediately for the reason of 'Key Compromise.'
- If a Subscriber's Token is lost or stolen, then all Subscriber Certificates associated with that Token shall be revoked immediately for the reason of 'Key Compromise.'
- When a Certificate is revoked for the reason of Key Compromise, the derivative Certificates (i.e., Certificates issued based on the compromised Certificate) shall also be revoked. If it is determined that a Private Key used to authorize the issuance of one or more Certificates may have been compromised, all Certificates directly or indirectly authorized by that private key since the date of the actual or suspected Compromise shall be revoked or shall be verified as appropriately issued.

In all other cases, Revocation of the Certificates is mandatory.

Where a Subscriber's Certificate is revoked, the Revocation shall be published in the appropriate CRL.

In the case of a CA Certificate issued by a Root, Principal or Subordinate CA may need to be revoked, the OA shall seek guidance from the PMA before Revocation of the Certificate except when the PMA is not available and there is an emergency such as:

- Request from the Subject CA for reason of Key Compromise;
- Determination by the OA that a Subject CA key is compromised; or
- Determination by the OA that a Subject CA is in violation of this CP, an applicable CPS, or a contractual obligation to a degree that threatens the integrity of the PKI.

Revocation Request Grace Period

This CP does not allow a Revocation grace period. Responsible parties shall request Revocation as soon as they identify the need for Revocation.

Time within which CA must Process the Revocation Request

For the CA, all Revocation requests shall be processed within 24 hours of receipt of request.

Online CAs shall revoke Certificates before the next CRL is published, except when the request is validated within two hours of CRL issuance. Revocation requests validated within two hours of CRL issuance shall be processed before the following CRL is published.

Revocation request processing time shall be as specified below:

Assurance Level	Processing Time for Revocation Requests
Low Assurance	Within 24 hours of receipt of request
Medium	Before next CRL is generated unless request is received within two (2) hours of CRL generation.

Revocation Checking Requirements for Relying Parties

Although the CRL issued by the CA has a validity period of 30 days, the Relying Party shall check for a refreshed CRL every 24 hours to obtain the latest Cross-Certificate Revocations reported.

Practice Note: *In any case, use of revoked Certificates could have damaging or catastrophic consequences in certain cases. The matter of how often new Revocation data should be obtained and whether to rely upon a Certificate whose Revocation status is temporarily unavailable is a determination to be made by the Relying Party, considering the Risk, responsibility, and consequences for using a Certificate whose Revocation status cannot be guaranteed.*

CRL Issuance Frequency

CAs shall issue CRLs, even when no changes have occurred. CRL issuance encompasses designating a CRL for activation, creation and publication to replace the previous CRL.

For the CA, the interval between CRLs shall not exceed the following:

Type of Issuance	Scope	CRL Issuance Frequency
Routine	Offline CAs that do not issue Subscriber Certificates except administration of the CA itself and CSA Certificates	when new record created or 1 year, whichever is earlier
	All other CAs	24 Hours
Emergency	CA Key Compromise	18 hours
	All other Key Compromise	Immediately, but no later than 18 hours

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

CRL issuance frequency requirements may be further constrained by applicable law. CAs are required to notify the OA upon Emergency CRL issuance for CA Key Compromise.

Maximum Latency of CRLs

CRLs shall be published within 4 hours of generation. Furthermore, each CRL shall be published no later than the time specified in the nextUpdate field of the previously issued CRL for same scope.

CAs shall coordinate with Repositories to reduce the latency between the moment the CA desires the CRL to be published and the moment the CRL is available to Relying Parties within the applicable Repositories.

The maximum latency between the moment a Revocation request is validated and the moment the Revocation information is published and available to Relying Parties shall be no greater than 24 hours.

On-line Revocation/Status Checking Availability

If On-line Revocation/status checking is supported by an CA, the latency of Certificate status information distributed on-line by CAs, or their delegated status responders shall meet or exceed the requirements for CRL issuance stated in Section 0.

On-line Revocation Checking Requirements

The CAs are responsible for updating and maintaining their OCSP responder entries in the OA's list and have sole discretion on which OCSP responders, if any, they desire to include in the OA's list.

The PKI Repository shall contain and publish a list of all OCSP Responders operated by the CAs.

Other Forms of Revocation Advertisements Available

A CA may also use other methods to publicize the Certificates it has revoked. Any alternative method shall meet the following requirements:

- The alternative method shall be described in the CA's approved CPS.
- The alternative method shall provide Authentication and Integrity services commensurate with the Assurance Level of the Certificate being verified.
- The alternative method shall meet the issuance and latency requirements for CRLs stated in Sections 0 and Sections 0.

A CA is not required to check for such forms of advertisements.

Special Requirements Related to Key Compromise

In the event of Compromise or suspected Compromise of the CA signing key, PMA, OA, Subscriber and any Cross Certified CAs shall be notified within 18 hours (See Section 4.9.7). Circumstances for Suspension

The CA shall not use suspension.

Who can Request Suspension

The CA shall not use suspension.

Procedure for Suspension / Un-Suspension Request

The CA shall not use suspension.

Limits on Suspension Period

The CA shall not use suspension.

4.10 CERTIFICATE STATUS SERVICES

All Certificate Status Services such as SCVP or OCSP for all Subscriber certificates for other Assurance Levels and all other CA certificates is optional.

Operational Characteristics

Certificate Revocation status shall be ascertained by querying the CRL maintained and published in its Repository by the CA, or by querying an OCSP Responder operated by the CA, if present.

Service Availability

Relying Parties are bound to their obligations and the stipulations of this CP irrespective of the availability of the Certificate Status Service.

For the CA, mechanisms and procedures shall be designed to ensure Certificate Status Services are available for use 24 hours a day, 7 days a week, with a minimum of 99% availability overall per year.

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.

A Subscriber may terminate his subscription either by allowing his Certificate to expire without Renewing or re-keying it, or by revoking his Certificate before expiry without applying for a replacement.

4.12 KEY ESCROW AND RECOVERY

Key Escrow and Recovery Policy and Practices

The CA shall not perform any escrow or key recovery functions.

For CAs, neither CA Private Keys, End-Entity, nor Subscriber signature keys shall be escrowed.

If Subscriber encryption keys are escrowed, policies and practices guiding this operation shall be documented either by:

- adopting the Key Recovery Policy (KRP) and developing a Key Recovery Practice Statement (KRPS); or
- developing a KRP that establishes security and authentication requirements comparable to an existing FAA KRP and developing a KRPS describing the procedures and controls implemented to comply with the KRP. The KRP may be a separate document or combined with the CP.

The KRPS may be a separate document or combined with the CPS.

Key Recovery policies and practices shall satisfy Privacy and security requirements (See Section 9.4) for CAs issuing and managing digital Certificates under the CP.

In either case, an independent compliance auditor under the following circumstances shall analyze the Key Escrow practices in the KRPS or CPS for compliance with the KRP:

Circumstance	Key Escrow and Recovery Applicability
Private Key Corresponding to a Human Subscriber Encryption Certificate	Key Escrow and Recovery is mandatory.
Private Key Corresponding to an NPE Subscriber Encryption Certificate	Key Escrow and Recovery is mandatory unless the data protected by the keys shall not require recovery under any circumstances.

Session Key Encapsulation and Recovery Policy and Practices

Entity CAs that support session key encapsulation and recovery policies and practices shall be identified in the Key Recovery Policy (KRP) or combined CP/KRP, and the Key Recovery Practice Statement (KRPS) or combined CPS/KRPS.

5. FACILITY, MANAGEMENT AND OPERATIONS CONTROLS

5.1 PHYSICAL CONTROLS

Site Location and Construction

The location and construction of the facility housing CA 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, High security locks, and intrusion sensors, shall provide robust protection against unauthorized access to CA equipment and records.

The workstation of remote administrators of the CA shall be located such that all accesses may be logged and monitored, and that there is a reasonable expectation that it would be impossible for a determined unauthorized individual to gain access to the workstation.

Virtual Machine Environments are permitted, but shall be limited to Hypervisor type virtual environments and be subject to all physical and logical controls described in this CP.

Physical Access

CA, CSA, and Signature Trust Platform (STP) equipment, including remote workstations used to administer the CAs, shall always be protected from unauthorized access. The security mechanisms shall be commensurate with those used to house high value, sensitive information.

5.1.1.1 Physical Access for CA Equipment

The physical security requirements pertaining to CA, and STP equipment shall:

- Ensure no unauthorized access to the hardware shall be permitted.
- Ensure all removable media and paper containing sensitive plain-text information shall be stored in secure containers.
- Ensure manual or electronic monitoring for unauthorized intrusion at all times.
- Ensure an access log shall be maintained and inspected periodically.
- Require Two-Person physical access control to both the Cryptographic Module and computer systems.
- Provide at least three layers of physical access boundaries (e.g., perimeter, building, PKI room).

Removable Cryptographic Modules shall be deactivated prior to storage. When not in use, Cryptographic Modules, activation information used to access or enable Cryptographic Modules, and other sensitive CA equipment 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, 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").
- Off-line CA equipment is shut down or HSMs are deactivated and securely stored.

- Any security containers are properly secured.
- Physical security systems (e.g., door locks, vent covers) are functioning properly,
- The area is secured against unauthorized access.

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

5.1.1.2 Physical Access for RA Equipment

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

5.1.1.3 Physical Access for CSA Equipment

Physical access control requirements for CSA equipment (if implemented), shall meet the CA physical access requirements specified in Section 5.1.1.1.

Power and Air Conditioning

CAs, and CSAs shall have backup capability sufficient to automatically lock out input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown.

Repositories shall be provided with uninterrupted power sufficient for a minimum of six hours operation in the absence of commercial or line power.

Water Exposures

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

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

The Operator shall ensure that CA and CSA records and documentation are protected from water exposure.

Fire Prevention and Protection

The CA Operator shall ensure the CA and CSA are protected by a fire suppression system.

Media Storage

CA and CSA media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic) and unauthorized physical access.

Media that contains audit, Archive, or Backup information shall be duplicated and stored in a location separate from the CA and CSA location.

Waste Disposal

Sensitive media and documentation that are no longer needed for operations shall be destroyed in a secure manner. For example, sensitive paper documentation shall be shredded, burned, or otherwise rendered unrecoverable.

Off-Site Backup

CA and CSA shall create and periodically test full system Backups sufficient to recover full PKI services from a system failure. Backups are to be performed and stored off-site not less than once every seven days. At least one full backup copy shall be stored at an off-site location separate from the CA equipment. Only the latest full Backup need to be retained. The Backup shall be stored at a site with physical and procedural controls commensurate to that of the operational CA and CSA.

5.2 PROCEDURAL CONTROLS

Corporate Controls

No Stipulation.

Trusted Roles

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 defined in terms of four roles. (Note: the information derives from the Certificate Issuing and Management Components (CIMC) Protection Profile.)

1. System Administrator – authorized to install, configure, and maintain the CA; establish and maintain user accounts; configure profiles and Audit parameters; and generate component keys.
2. Audit Administrator – authorized to maintain audit logs.
3. Operator – authorized to perform system backup and recovery.
4. Registration Authority – authorized to request or approve Certificates or Certificate Revocations.

The following subsections provide a detailed description of the responsibilities for these primary trusted roles and secondary trusted roles.

5.2.1.1 CA Systems Administrator

The CA System administrator shall be responsible for:

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

CA System Administrators shall not issue Certificates to Subscribers.

5.2.1.2 Audit Administrator or Auditor

The auditor role shall be responsible for:

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

5.2.1.3 CA Operator

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

5.2.1.4 Registration Authority

The Registration Authority shall be responsible for issuing Certificates, that is:

- Registering new Subscriber Applicants and requesting the issuance of Certificates.
- Verifying the identity of Subscribers and accuracy of information included in Certificates.
- Approving and executing the issuance of Certificates,
- Receiving and distributing Subscriber Certificates.
- Securely communicating requests to and responses from the CA; and
- Requesting, approving and executing the Revocation of End-Entity 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.

Practice Note: *For the purposes of this CP, Registration Authority may be construed as a PKI system entity (See section 1.3.2) and a trusted role person (this section). They are separate and distinct PKI components.*

5.2.1.5 CSA Roles

A CSA shall have at least the following roles:

The CSA Administrator shall be responsible for:

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

The CSA Auditor shall be responsible for:

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

The CSA Operator shall be responsible for:

- The routine operation of the CSA equipment.

- Operations such as system Backups and recovery or changing recording media.

5.2.1.6 CMS Roles

The CMS is not applicable for the NPE-IDMS CA.

A CMS shall have at least the following roles:

The CMS Administrator shall be responsible for:

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

The CMS Auditor 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.

The CMS Officer shall be responsible for issuing Certificates, that is:

- Registering new Subscribers and requesting the issuance of Certificates;
- Verifying the identity of Subscribers and accuracy of information included in the Certificate Request;
- Approving the issuance of Certificates; and.
- Requesting and approving the Revocation of Certificates.

Practice Note: *The CMS Officer plays the role of the RA.*

5.2.1.7 Device Sponsor

A Device Sponsor shall fill the role of a Subscriber for NPEs that are named as Public Key Certificate Subjects. The Device Sponsor works with the RAs to register components (e.g., routers, Firewalls, etc.) and is responsible for meeting the obligations of Subscribers as defined throughout this document.

Device Sponsor need not be a Trusted role (that would be subject to the requirements for Sections 5.2.2.1, 5.2.2.3, 5.2.2.4, 5.2.2.5 and all sections within 5.3) but shall have a credential that is equal to or Higher Assurance Level than the credential that they are sponsoring.

5.2.1.8 Trusted Agent

A Trusted Agent shall be responsible for:

- Verifying identity, and

- Securely communicating Subscriber information to the RA.

A Trusted Agent is **NOT** a Trusted Role.

5.2.1.9 Role Sponsor

A Role Sponsor shall be a Subscriber responsible for the management activities pertaining to the Roles Certificates for which they are the sponsor. The Role Sponsor shall hold an individual Certificate in their own name issued by the same CA at the same or higher Assurance Level as the Role Certificate being requested for Subscribers. The Role Sponsor need not hold a Role Certificate.

In addition, the Role Sponsor shall be responsible for:

- Authorizing individuals for a Role Certificate.
- Recovery of private decryption keys associated with Role Encryption Certificates.
- Revocation of individual Role Certificates.
- Always maintaining a current up-to-date list of individuals who have been issued Role Certificates.
- Always maintaining a current up-to-date list of individuals who have been provided decryption Private Keys associated with Role Encryption Certificates.

A Role Sponsor is NOT a Trusted Role.

Number of Persons Required per Task

The CA and CSA shall ensure a separation of duties into trusted roles for critical CA functions to prevent one CA staff member from maliciously using the CA system without detection. Each such trusted role's system access is to be limited to those actions they are required to perform in fulfilling their responsibilities.

A CA and CSA shall ensure that no single individual may gain access to its Private Key.

Two or more persons are required for the following tasks:

- CA and CSA Key Generation.
- CA and CSA signing Key Activation.
- CA and CSA private Key Backup.

Where multiparty control for logical access 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. Multiparty control for logical access shall not be achieved using personnel that serve in the Auditor Trusted Role.

Identification and Authentication for Each Role

An individual in a trusted role shall identify and authenticate themselves before being permitted to perform any actions set forth above for that role or identity. Specifically, these actions include being:

- included in the access list for the CA and CSA Secure Area; and
- included in the access list for the CA and CSA System; and
- given a Certificate for the performance of their CA and CSA role; and
- given an account on the PKI system.

Each of these Certificates and accounts (with the exception of the CA and CSA signing Certificates) shall:

- Be directly attributable to an individual.
- Not be shared.
- Be restricted to actions authorized for that role through the use of CA and CSA software, operating system and procedural controls.
- Limit Operations to being performed at the console of the CA and CSA computer system.

An individual in a Trusted Role shall authenticate to remote components of the PKI using a method commensurate with the strength of the PKI.

Roles Requiring Separation of Duties

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

The CA and RA software and hardware shall identify and authenticate its users and shall ensure that no user identity can assume both an Administrator and an RA role, assume both the Administrator and Auditor roles, and assume both the Auditor and RA role.

Requirements for the separation of roles, and limitations on use of procedural mechanisms to implement role separation are as follows:

Individual personnel shall be specifically designated to the four roles defined in Section 5.2.2 above.

- Individuals who assume an Auditor role shall not assume any other role.
- Individuals who assume an RA role shall not assume an Auditor or Administrator role.
- No individual in a trusted role shall have more than one identity.

Practice Note: *Persons in auditor role may perform Backups limited to the audit logs and Archive without being categorized as being in an operator trusted role.*

5.3 PERSONNEL CONTROLS

Background, Qualifications, Experience, & Clearance Requirements

The FAA shall identify the set of individuals assigned to primary and secondary trusted roles, who are responsible and accountable for the operation of each CA, CSA, and RA.

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity. Personnel appointed to trusted roles shall:

- Have an active PIV card issued by the FAA.
- Have successfully completed an appropriate training program.
- Possess the expert knowledge, experience and qualifications necessary for the offered services and appropriate for the job function.
- Have no other duties that would interfere or conflict with their duties for the trusted role.
- Be trustworthy;

- Have not been previously relieved of duties for reasons of negligence or non-performance of duties;
- Have not been denied a security clearance or had a security clearance revoked for cause;
- Have not been convicted of a felony, a serious crime or other offense which affects his/her suitability for the position
- Be appointed in writing by an approving authority.

For CAs issuing Certificates equal to or higher than *Medium* Assurance Level, each person filling a trusted role shall also satisfy at least one of the following:

- The person shall be a citizen of the country where the CA is located; or
- For CAs operated on behalf of multinational governmental organizations, the person shall be a citizen of one of the member countries; or
- For CAs located within the European Union, the person shall be a citizen of one of the member States of the European Union.

If a given CA only operates at the *Low* Assurance Level, it is permissible for the trusted roles for that CA not to have qualification beyond those normally applied to hiring Employees of the FAA, or of those normally stipulated for FAA contractors, providing that any such trusted roles do not have any access, privilege or permission on any CA operating at any other Assurance Level higher than Low, and that any component of the *Low* Assurance Level CA does not share a physical or logical location with a CA of a Higher Assurance Level.

Background Check Procedures

Inherited from FAA ASH Program.

Training Requirements

All individuals in trusted roles shall receive comprehensive training in all operational duties they are expected to perform prior to being allowed to act in the role. Training shall cover the following:

- CA, CSA and RA Security principles and mechanisms.
- All PKI software versions in use by the individual in the trusted role.
- All duties the individual is expected to perform.
- Disaster recovery and business continuity procedures.

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

Retraining Frequency and Requirements

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

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

A reasonable effort shall be made to ensure all staff review the documentation and procedures pertaining to their job function on an annual basis.

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

Job Rotation Frequency and Sequence

The entity CA shall implement job rotation to enable redundancy for all roles while maintaining segregation of duties. Corrective Action for Unauthorized Actions

The PMA shall take appropriate actions where personnel have performed actions not authorized in this CP.

In the event of actual or suspected unauthorized action by a person performing duties with respect to the operation of a CA, CSA or RA, the CA shall suspend his or her access pending outcome of the investigation and take appropriate corrective action if deemed necessary.

Independent Contractor Requirements

Contractor personnel employed to perform trusted role functions shall meet the personnel requirements set forth in Section 5.3 as applicable.

Documentation Supplied To Personnel

For the CA, documentation sufficient to define duties and procedures for each trusted role shall be provided to the personnel filling that role. The documentation and procedures shall include the applicable portions of the CP and CPS, relevant statutes, policies or contracts, and other technical, operations and administrative documents (e.g., Administrator Manual, User Manual, etc.) as applicable.

5.4 AUDIT LOGGING PROCEDURES

Audit log files shall be generated for all events relating to the security of the CAs, CSAs, RAs and STPs. For CAs operated in a virtual machine environment (VME), audit logs shall be generated for all applicable events on both the virtual machine (VM) and isolation kernel (i.e., Hypervisor).

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 and per Section 5.5.2.

Types of Events Recorded

All security auditing capabilities of the CA, CSA, RA, and STP operating systems and CA, CSA, RA, STP applications required by this CP shall be enabled. As a result, most of the events identified in the table shall be automatically recorded. Where events cannot be automatically recorded, the CA shall implement manual procedures to satisfy this requirement.

At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- The type of event.
- The date and time the event occurred.

- A success or failure indicator, where appropriate.
- The identity of the entity and/or operator that caused the event.
- A message from any source received by the CA requesting an action related to the operational state of the CA is an auditable event.

The following events shall be audited:

Auditable Event	CA	CSA	RA	STP
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 timestamp	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 maximum authentication attempts 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
LOCAL DATA ENTRY				
All security-relevant data that is entered in the system	X	X	X	X
REMOTE DATA ENTRY				
All security-relevant messages that are received by the system	X	X	X	X
DATA EXPORT AND OUTPUT				
All successful and unsuccessful requests for confidential and security-relevant information	X	X	X	X
KEY GENERATION				

Whenever the Component generates a key (not mandatory for single session or one-time use symmetric keys)	X	X	X	X
PRIVATE KEY LOAD AND STORAGE				
The loading of Component Private Keys	X	X	X	X

Auditable Event	CA	CSA	RA	STP
All Access to Certificate Subject Private Keys retained within the CA for key recovery purposes	X	N/A	N/A	X
TRUSTED PUBLIC KEY ENTRY, DELETION, AND STORAGE				
All changes to the trusted Component Public Keys, including additions and deletions	X	X	X	X
SECRET KEY STORAGE				
The manual entry of secret keys used for authentication	X	X	X	X
PRIVATE AND SECRET KEY EXPORT				
The export of private and secret keys (keys used for a single session or message are excluded)	X	X	X	X
CERTIFICATE REGISTRATION				
All Certificate Requests	X	N/A	X	X
CERTIFICATE REVOCATION				
All Certificate Revocation requests	X	N/A	X	X
CERTIFICATE STATUS CHANGE APPROVAL				
The approval or rejection of a Certificate status change request	X	N/A	N/A	X
CA CONFIGURATION				
Any security-relevant changes to the configuration of the Component	X	X	X	X

ACCOUNT ADMINISTRATION				
Roles and users are added or deleted	**X**	**N/A**	**N/A**	**X**
The access control privileges of a user account or a role are modified	**X**	**N/A**	**N/A**	**X**
CERTIFICATE PROFILE MANAGEMENT				
All changes to the Certificate profile	**X**	**N/A**	**N/A**	**X**
CERTIFICATE STATUS AUTHORITY MANAGEMENT				
Auditable Event	**CA**	**CSA**	**RA**	**STP**
All changes to the CSA profile (e.g., OCSP profile)	**N/A**	**X**	**N/A**	**N/A**
REVOCATION PROFILE MANAGEMENT				
All changes to the Revocation profile	**X**	**N/A**	**N/A**	**N/A**
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT				
All changes to the Certificate Revocation List profile	**X**	**N/A**	**N/A**	**N/A**
MISCELLANEOUS				
Appointment of an individual to a trusted role	**X**	**X**	**X**	**X**
Designation of personnel for multiparty control	**X**	**N/A**	**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 Start-up	**X**	**X**	**X**	**X**
Login 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 database	**X**	**N/A**	**N/A**	**X**
Restoration from back up of the internal database	**X**	**N/A**	**N/A**	**X**
File manipulation (e.g., creation, renaming, moving)	**X**	**N/A**	**N/A**	**N/A**
Posting of any material to a PKI Repository	**X**	**N/A**	**N/A**	**N/A**

Auditable Event	CA	CSA	RA	STP
Access to the internal CA database	X	X	N/A	N/A
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 Tokens	X	N/A	X	X
Re-key of the Component	X	X	X	X
CONFIGURATION CHANGES				
Hardware	X	X	N/A	X
Software	X	X	X	X
Operating system	X	X	X	X
Patches	X	X	N/A	X
Security profiles	X	X	X	X
PHYSICAL ACCESS / SITE SECURITY				
Personnel Access to room housing Component	X	N/A	N/A	X
Access to the Component	X	X	N/A	X
Known or suspected violations of physical security	X	X	X	X
ANOMALIES				
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

1731

Auditable Event	CA	CSA	RA	STP
Equipment failure	X	N/A	N/A	X
Electrical power outages	X	N/A	N/A	X
Uninterruptible Power Supply (UPS) failure	X	N/A	N/A	X
Obvious and significant network service or access failure	X	N/A	N/A	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

Frequency of Processing Log

Audit logs shall be reviewed at least once every month, except for off-line CAs where the review shall be performed at least once a year or when the system is activated, whichever is shorter. The process and details of the review shall be detailed in the CPS.

In any event, 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 log entries, with a more thorough investigation of any alerts or irregularities in the logs. Examples of irregularities include discontinuities in the logs and loss of audit data.

A statistically significant sample of security audit data generated by CA, CSA, RA, and STP 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.

Significant events and actions taken as a result of these reviews shall be documented.

The Audit Administrator shall explain all significant events in a monthly audit log summary.

Retention Period for Audit Logs

Audit logs shall be retained on-site for at least sixty (60) days or until it is reviewed if the review happens after 60 days; as well as being retained in the manner described below.

For CA, CSA, and STP, the individual who removes audit logs, either directly or through supervision, shall be an Audit Administrator. For an RA, the individual who removes audit logs shall be a System Administrator who is not an RA.

Protection of Audit Logs

For *Medium* assurance or Higher, system configuration and procedures shall be implemented together to ensure that:

- Only personnel assigned to the appropriate Trusted Roles have read access to the logs (see Section 5.4.3).
- Only authorized people may archive audit logs.
- Audit logs are not modified or destroyed.

The person performing audit log Archive need not have modify access, but procedures shall be implemented to protect archived data from destruction prior to the end of the audit log retention period (note that deletion requires modification access).

The off-site storage location for audit logs shall be a safe, secure location separate from the location where the data was generated.

This process shall be documented in the CPS.

Practice Note: *It is acceptable for the system to overwrite audit logs after they have been backed up and Archived.*

Audit Log Backup Procedures

For on-line CAs, at least every 30 days for components operating at *Medium* assurance and Higher Assurance Levels, audit logs shall be backed up or copied if in manual form and stored in an off-site secure facility.

For off-line CAs audit logs backup shall be backed up or copied in manual form stored in an off-site secure facility and be performed once a month or when the system is activated, whichever is longer.

With sufficient system redundancy in place, Backups for the offline CAs shall be performed at least every three months.

A copy of the audit log shall be sent off-site on a monthly basis or at the next Backup for off-line CAs.

Audit Collection System (internal vs. external)

The audit log collection system may or may not be external to the CA, CSA, STP, or RA system. Automated audit processes shall be invoked at system (or application) startup and cease only at system (or application) 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 its operation until the problem is remediated.

Notification to Event-Causing Subject

This CP imposes no requirement to provide notice that an event was audited to the individual or NPE (Sponsor, Organization, Device, or application, etc.) that caused the event.

Vulnerability Assessments

A Vulnerability Assessment including the enclave containing the PKI components (CA, CSA, RA and Hypervisor) shall be carried out at least once a year and use Doc 10204 – Manual on Information Security as the standard against which the entity PKI is assessed..

5.5 RECORDS ARCHIVE

CA, CSA, STP, and RA archive records shall be sufficiently detailed as to verify that the PKI was properly operated, as well as verify the validity of any Certificate (including those revoked or expired) issued by the CA.

Types of Events Archived

At a minimum, the following data shall be recorded for Archive in accordance with each Assurance Level:

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

Data to be Archived	**Root CA/ CA**	**CSA**	**RA**	**STP**
Certificate Policy	x/x	x	x	x
Certification Practice Statement	X/X	X	X	X
Contractual obligations	X/X	X	X	X
System and equipment configuration	X/X	X	N/A	X
Modifications and updates to system or configuration	X/X	X	N/A	X
Certificate Requests	X/X	N/A	N/A	X
Revocation Requests	X/X	N/A	N/A	X
Subscriber identity authentication data as per Section 3.2.3	N/A / X	N/A	X	X
Documentation of receipt and acceptance of Certificate	X/X	N/A	X	X
Signed Subscriber Agreements	N/A /X	N/A	X	X
Documentation of receipt of Tokens	N/A / X	N/A	X	X
All Certificates issued or published	X/X	N/A	N/A	X
Record of Component CA Re-key	N/A / N/A	X	X	X
All CRLs and CRLs issued and/or published	X/X	N/A	N/A	N/A
All Audit logs	X/X	X	X	X
Other data or applications to verify Archive contents	X/X	X	X	X

Documentation required by Compliance Auditors	X/X	X	X	X
External Compliance Audit or Internal Audit Reports	X /X	X	X	X

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 and the applications required to process it shall be retained for the longer of 10 years and 6 months and the applicable record retention laws (see Section 9.17.5) in the CAs chosen jurisdiction. Where the retention period is longer than 10 years and 6 months the applicable CP or CPS shall state the retention period as required in 9.17.5.

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

Applications required for processing the archive data shall also be maintained for the minimum retention period specified above. The FAA may retain data using whatever procedures have been approved by the U.S. National Archives and Records Administration or by the respective records retention policies in accordance with whatever laws apply to those entities for that category of documents.

Protection of Archive

The CA shall:

- prevent unauthorized user access to the Archive to write to, modify, or delete the Archive (for CA, and CSA only the Audit Administrators shall be authorized and for RA, someone other than an RA role shall be permitted (e.g., ISSO).
- prevent release of the contents of the Archive, except as determined by the PMA for the CA or as required by law.
- allow release of records of individual transactions upon request of any Subscribers involved in the transaction or their legally recognized agents.
- Ensure that the archived data are protected in accordance with the privacy laws of the country in which the Subscriber information was collected and any applicable privacy laws from the Subscriber's citizenship country.

Archive Backup Procedures

Adequate and regular Backup procedures shall be in place so that in the event of loss or destruction of the primary Archives, a complete set of Backup copies held in a separate location shall be readily available in a short period of time.

The CPS or a referenced document shall describe procedures for how the records are backed up and how the archive Backups are managed.

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.

Archive Collection System (Internal or External)

No stipulation.

Procedures to Obtain and Verify Archive Information

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

The archived data shall be protected in accordance with the privacy laws of the country in which the Subscriber information was collected and any applicable privacy laws from the Subscriber's citizenship country.

The contents of the Archive shall not be released except in accordance with Sections 9.3 and 9.4.

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, Public Key shall be available to verify old signatures until all the Certificates signed using the associated Private Key have also expired. If the old Private Key is used to sign CRLs that cover Certificates signed with that key, then the old key shall be retained and protected.

The maximum lifetimes for Certificates and associated Private Keys can be found in section 6.3.2 Certificate Operational Periods/Key Usage Periods table.

A CA cannot generate a Certificate for a Subscriber whose validity period would be longer than the CA Certificate validity period. The CA Key Pair shall be changed prior to the end of the validity period of the CA Certificate in time to ensure that no Certificate issued by the CA asserts a validity period that extends beyond the validity period of the CA Certificate.

Practice Note: *CA software may automatically shorten the validity period of a Subscriber Certificate such that it will not extend beyond the CAs Certificate validity period.*

CAs shall describe their key changeover procedures in the applicable CPS. Key changeover procedures shall establish Key Rollover Certificates where a Certificate containing the old Public Key shall be signed by the new Private Key, and a Certificate containing the new Public Key shall be signed by the old Private Key.

After a CA performs a Key Changeover, the CA may continue to issue CRLs with the old key until all Certificates signed with that key have expired. As an alternative, after all Certificates signed with that old key have been revoked, the CA may issue a final long-term CRL using the old key, with a nextUpdate time passed the validity period of all issued Certificates. This final CRL shall be available for all relying parties until the validity period of all issued Certificates has passed. Once the last CRL has been issued, the old private signing key of the CA may be destroyed.

5.7 COMPROMISE AND DISASTER RECOVERY

Incident and Compromise Handling Procedures

If a CA or CSA detects a potential penetration or other form of Compromise, it shall perform an investigation to determine the nature and extent of damage. If a CA or CSA key is suspected of Compromise, the procedures in Section 0 shall be followed. Otherwise, the damage shall be assessed to determine if the remediation required shall be to rebuild the impacted CA or CSA or components thereof, revoke a set of Certificates, and/or declare a CA or CSA Key Compromise.

If the issuance of an unauthorized certificate from any CA is detected, the unauthorized certificate shall be revoked, and the certificate issuance capability of the CA shall be suspended. A security investigation shall be initiated to determine the cause and the results shall be reported to the FAA.

The CA shall notify the members of the PMA and all parties with direct trust with the CA, if any, of the following incidents occur:

- suspected or detected Compromise of the CA systems.
- physical or electronic attempts to penetrate CA systems.
- denial of service attacks on CA components.
- any incident preventing the CA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL.

The PMA shall provide further notice to all cross-certified members of the CA to ensure that other PKI domains can protect their interest as Relying Parties.

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

In the event of an incident as described above, the OA Administrator shall notify the PMA within 24 hours of incident discovery, along with preliminary remediation analysis. Within 10 business days of incident resolution, FAA shall post a notice on its public web page identifying the incident. The public notice shall include the following:

- Which CA components were affected by the incident?
- The CA's interpretation of the incident.
- Who is impacted by the incident?
- When the incident was discovered.
- A complete list of all Certificates that were either issued erroneously or not compliant with the CP/CPS as a result of the incident.
- A statement that the incident has been fully remediated.

The notification provided directly to the PMA and other direct trust members shall also include detailed measures taken to remediate the incident.

CAs shall provide notice whenever the Revocation of a Cross-Certificate is planned.

The OA, shall be notified if any of the following cases occur:

- Revocation of a relevant CA Certificate, such as for a CA cross-certified with the other domain’s PKI, is planned; or

any incident preventing such a relevant CA from issuing a CRL within twenty-four (24) hours of the time specified in the next update field of its currently valid CRL. The CA Operational Authority shall re-establish operational capabilities as quickly as possible in accordance with procedures set forth in the respective CPS.

The Entity STP shall have documented incident-handling procedures that are approved by the person responsible for operating the Entity STP. If the STP or Entity STP keys are compromised, all *TSP Mediated Signature* Certificates issued to the entity STP shall be revoked. The damage caused by the Entity STP Compromise shall be assessed and all Subscriber Certificates that may have been compromised shall be revoked, signature proofs shall be destroyed, and Subscribers shall be notified of such Revocation. The Entity STP shall be re-established.

Computing Resources, Software, and/or Data Are Corrupted

When CA or CSA computing resources, software, and/or data are damaged, rendered inoperative or corrupted, the CA or CSA shall respond as follows:

- If the CA signature keys are not destroyed**,** CA operation shall be reestablished as quickly as possible, giving priority to the ability to generate Certificate status information.
- Before returning to operation, a system's integrity check shall be performed.
- If a CA cannot issue a CRL prior to the time specified in the next update field of its currently valid CRL, then all CAs that have been issued Certificates by the CA shall be securely notified immediately. This will allow other CAs to protect their Subscribers' interests as Relying Parties.
- If the ability to revoke Certificates is inoperable or damaged, the CA shall re-establish Revocation capabilities as quickly as possible in accordance with procedures set forth in the applicable CPS.
- If the CA's Revocation capability cannot be recovered in a reasonable timeframe, the CA shall determine whether to request Revocation of its Certificate(s). If the CA is a Root CA, the CA shall determine whether to notify all Subscribers that use the of CA as a trust anchor is no longer appropriate.

The OA shall post a notice on its web page identifying the incident and notify all direct trust entities as per Section 5.7.1.

Private Key Compromise Procedures

The Subscriber shall report any suspected or real compromise of their Private Key to their Issuing CA or RA.

If a CA signature key is compromised or lost (such that compromise, or loss is possible even though not certain):

- The CA shall securely notify the PMA and all cross-certified entities so that entities may issue CRLs revoking any Cross-Certificates issued to the compromised CA.
- A new CA Key Pair shall be generated by the CA in accordance with procedures set forth in the applicable CPS.
- New CA Certificates shall be issued to Entities in accordance with this CP.
- The CA shall request all Subscribers to Re-key using the procedures outlined in Section 3.3.2.
- If the CA distributes its key in a self-signed Certificate (e.g., Root CA), the new self-signed Certificate shall be distributed as specified in Section 0.
- The CA PMA shall also investigate what caused the compromise or loss, and what measures shall be taken to preclude recurrence.

For those Certificate Requests or approvals that cannot be ascertained as legitimate, the resultant Certificates shall be revoked and their Subjects (i.e., Subscribers) shall be notified of Revocation.

If a CSA signature key is compromised, suspected of being compromised or lost:

- All Certificates issued to the CSA shall be revoked.
- The CSA shall generate a new Key Pair and request new Certificates, if applicable.
- If the CSA is a trust anchor, Relying Parties shall be provided a new trust anchor in a secure manner as a replacement for the compromised trust anchor.

If a RA signature key is compromised or lost (such that compromise, or loss is possible even though not certain):

- The RA Certificate shall be revoked immediately.
- A new RA Key Pair shall be generated according to the applicable CPS.
- A new RA Certificate shall be requested according to the applicable CPS.
- All Certificate Requests approved by the RA since the data of the suspected compromise shall be reviewed to identify inappropriate Certificate lifecycle actions which were a result of the compromise.
- For those Certificate Requests or approvals that cannot be ascertained as legitimate, the resultant Certificates shall be revoked and their Subjects (i.e., Subscribers) shall be notified of both the inappropriate action(s) and of Revocation. The CA shall post a notice on its web page describing the compromise (see Section 5.7.1 for contents of the notice).

Business Continuity Capabilities after a Disaster

In the case of a disaster whereby all of a CA's installations are physically damaged and all copies of the CA Signing Key are destroyed as a result, the CA Operator shall provide an alternate secure facility that conforms to all provisions of the present document for resumption of the CA following any CA service interruption and shall follow the requirements for Key Compromise as defined in Section 0.

5.8 CA, CSA, STP OR RA TERMINATION

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

Prior to CA termination, the OA shall provide all archived data to an archival facility. Any issued certificates that have not expired, shall be revoked and a final long term CRL with the nextUpdate time past the validity period of all issued certificates shall be generated. This final CRL shall be available for all relying parties until the validity period of all issued certificates has passed. Once the last CRL has been issued, the private signing key(s) of the entity CA shall be destroyed.

The OA shall be given as much advance notice as circumstances permit and attempts to provide alternative sources of interoperation shall be sought in the event the entity CA is terminated.

In the event of a Root CA or Subordinate CA termination, direct trust PKIs will be notified at least two (2) weeks prior to termination, if circumstances permit, an attempt 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.
- A CA, CSA, and RA archive records shall be transferred to an appropriate authority such as the PMA responsible for the entity.
- If a Root CA is terminated, that Root CA shall use secure means to notify the Subscribers to delete all trust anchors representing the terminated Root CA.

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

Key Pair Generation

Cryptographic key material shall be generated in validated Cryptographic Modules according to the following minimum requirements:

Entity Role / Certificate Profile	FIPS 140-2 Level or later	Hardware or Software	Key Storage Restricted to the Module on which the Key Was Generated
CA	**3**	**Hardware**	**Yes**
STP	**3**	**Hardware**	**Yes**
CSA (e.g., OCSP, SCVP)	**2**	**Hardware**	**Yes**
RA	**2**	**Hardware**	**Yes**
MediumHardware	**2**	**Hardware**	**Yes, for all Certificate profiles except for Subscriber Encryption**
MediumDevice	**1**	**Software**	**No**
LowTSP	**No requirement**	**Software /Hardware**	**No**
LowDevice	**No requirement**	**Software /Hardware**	**No**

Practice Note: *For MediumHardwareDevice: For Aircraft Signature, Aircraft Authentication, and Aircraft Encryption Certificates, a formal certification to FIPS 140-2 Level 2 is not required, provided that compliance with the security objectives of FIPS 140-2 Level 2 is demonstrated.*

Practice Note: *For MediumDevice, when using commercially available cryptography such as Microsoft crypto, bouncy castle, openssl, their certification can be considered equivalent.*

Random numbers shall be generated within FIPS 140 Level 2 validated hardware Cryptographic Modules for *MediumHardwareDevice* Assurance Levels.

When Private Keys are not generated on the Cryptographic Module to be used, originally generated Private Keys shall be destroyed after they have been transferred to the replacement Cryptographic Module unless the key generating module acts as the key escrow module. After the originally generated private keys are destroyed, the key generating module may be repurposed.

For CA, Key Pair generation shall create a verifiable audit trail that the security requirements for key generation were followed. The documentation of the procedure shall be detailed enough to show that appropriate role separation was used.

For multiparty control requirements, see Section 0.

An auditor approved independent third party shall validate the execution of the Key Generation for CAs, CSA, and TSAs.

Practice Note: *This may be through witnessing Key Generation directly or by examining the signed and documented record of the Key Generation.*

Private Key Delivery to Subscriber

CAs shall generate their own Key Pair and therefore do not need Private Key delivery.

If Subscribers generate their own Key Pairs, then there is no need to deliver Private Keys, and this section does not apply.

When CAs or RAs generate keys on behalf of the Subscriber, then the Private Key shall be delivered securely to the Subscriber. Private Keys may be delivered electronically or may be delivered on a hardware Cryptographic Module. In all cases, the following requirements shall be met:

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

The CA (or RA) shall maintain a record of the Subscriber acknowledgement of receipt of the Cryptographic Module.

Public Key Delivery to Certificate Issuer

Where Key Pairs are generated by the Subscriber, or RA, 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.

CA Public Key Delivery to Relying Parties

When a CA updates its Signature Key Pair, the CA shall distribute the new Public Key in a secure fashion. The new Public Key may be distributed in a self-signed Certificate, in a Key Rollover Certificate, or in a new Certificate (e.g., Cross-Certificate) obtained from the issuer(s) of the current CA Certificate(s).

Self-signed Certificates shall be conveyed to relying parties in a secure fashion to preclude substitution attacks.

Acceptable methods for self-signed Certificate delivery include:

- The CA loading a self-signed Certificate onto Tokens delivered to Relying Parties via secure mechanisms.
- Secure distribution of self-signed Certificates through secure Out-of-Band mechanisms.

- Comparison of the hash of the self-signed Certificate against a hash value made available via authenticated Out-of-Band sources (note that hashes posted in-band along with the Certificate are not acceptable as an authentication mechanism); and
- Loading Certificates from web sites secured with a currently valid Certificate of equal or greater Assurance Level than the Certificate being downloaded. The web site Certificate shall not be issued by a CA subordinated to the self-signed CA.

Key rollover Certificates are signed with the CA's current Private Key, so secure distribution is not required.

Key Sizes

If the security of a particular algorithm becomes compromised, the entity PMA or OA

may require CAs to revoke affected certificates, according to Section 9.4 and applicable regulations.

All Certificates, CRL, OCSP Responses, and cryptographic network protocols (e.g., TLS) materially relied on or issued by the PKI shall use at a minimum the following key sizes and algorithms:

Cryptographic Function	Expires 1/1/2011 – 12/31/2030	Expires after 12/31/2030
Signing (per FIPS 186-5)	2048-bit, 3072-bit, 4096-bit RSA or higher Or 224-bit prime field or 233-bit binary field or 283 bit binary field ECDSA or higher	3072-bit, 4096-bit RSA or higher Or 256-bit prime field or 283-bit binary field ECDSA or higher
Asymmetric Encryption ** key agreement protocol ** (Per PKCS1 for RSA and per 800-56A for ECDH)	2048-bit RSA or higher Or 224-bit prime field or 233-bit binary field ECDH or higher	3072-bit RSA or higher Or 256-bit prime field or 283-bit binary field ECDH or higher
Symmetric Encryption	AES-256 or higher	AES -256 or higher

The hashing algorithm used for Certificates, CRL, and OCSP Responses shall meet the following minimum requirements:

Scope	Issued 1/1/2011 - 12/31/2030	Issued after 12/31/2030
Certificates	SHA-224, SHA-256 or higher	SHA-256 or higher

CRL	SHA-224, SHA-256 or higher	SHA-256 or higher
Pre-Signed OCSP Responses	SHA-224, SHA-256 or higher	SHA-256 or higher
Non-Pre-Signed OCSP Reponses	SHA-224, SHA-256 or higher	SHA-256 or higher
CRLs, OCSP Reponses (pre-signed and non-pre-signed)	SHA-224,SHA-256 or higher	NA

CRLs, OCSP Responder Certificates, and OCSP Responses shall use the same or better signature algorithm, key size, and hash algorithm used for the Certificate that is being validated.

Public Key Parameters Generation and Quality Checking

RSA keys and prime numbers shall be generated and tested in accordance with FIPS 186-5.

ECDSA, EDDSA and ECDH keys shall be generated in accordance with FIPS 186-5. Curves referenced by FIPS 186-5 shall be used.

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

Public Keys that are bound into Certificates shall be certified for use in signing or encrypting, but not both, except as specified below. The use of a specific key is determined by the key usage extension in the X.509 Certificate. The following table describes the rules for asserting key usage extensions:

Human Subscriber or NPE	
Key Use	**Key Usage Extensions**
Human Identity NPE	Set: digitalSignature bit only Set: digitalSignature, keyEncipherment or keyAgreement Where RSA is used for DTLS or TLS, keyEncipherment shall be used. Where EC is used for DTLS or TLS, keyAgreement shall be used
Digital Signature	Set: digitalSignature, nonRepudiation bits Not Set: keyEncipherment, keyAgreement bits
Encryption	Set: keyEncipherment, dataEncipherment (optional)
Key Agreement	Set: keyAgreement
CA	
Key Use	**Key Usage Extensions**

Issuing Certificates	Set: cRLSign, keyCertSign bits
CSA	
Key Use	**Key Usage Extensions**
Signing OCSP Responses	Set: digitalSignature, nonRepudiation bits

Note: Where RSA is used for DTLS or TLS, keyEncipherment shall be used. Where EC is used for DTLS or TLS, keyAgreement shall be used.

If a Certificate is used for authentication of ephemeral keys, the Key Usage bit in the Certificate shall assert the digitalsignature and/or nonrepudiation bits and may or may not assert the Key Encryption and Key Agreement depending on the Public Key in the Certificate.

Extended key usage OIDs shall be consistent with the key usage bits set. See Section 10.22 for additional requirements pertaining to extended key usage.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

Cryptographic Module Standards and Controls

The relevant standard for Cryptographic Modules is FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*. The PMA may determine that other comparable and equivalent validation, certification, or verification international standards are sufficient.

Cryptographic Modules shall be validated to the FIPS 140-2 level identified in Section 0 or higher. Additionally, the PMA reserves the right to review technical documentation associated with any Cryptographic Modules under consideration for use by CAs.

6.2.1.1 Custodial Subscriber Key Stores

Custodial Subscriber Key Stores hold keys for a number of Subscriber Certificates in one location. When a collection of Private Keys for Subscriber Certificates are held in a single location, there is a Higher Risk associated with Compromise of that Cryptographic Module than that of a single Subscriber. Cryptographic Modules for Custodial Subscriber Key Stores at the *Low* Assurance Level shall be no less than FIPS 140 Level 1 (Hardware or Software). For all other levels, the Cryptographic Module shall be no less than FIPS 140 Level 2 Hardware. In addition, authentication to the Cryptographic device in order to activate the Private Key associated with a given Certificate shall require authentication commensurate with the Assurance Level of the Certificate.

Private Key Multi-Person Control

Use of a CA private signing key shall require action by multiple persons as set forth in Section 0 of this CP.

Private Key Escrow

Only Private Keys used for encryption shall be escrowed. .

End-Entity Private Keys used solely for decryption shall be escrowed prior to the generation of the corresponding Certificates, except for decryption Private Keys associated with aircraft and/or aircraft equipment Encryption Certificates which do not need to be escrowed. Furthermore, if the data protected by these decryption keys shall require recovery, such keys do not need to be escrowed.

Private Key Backup

6.2.1.2 Backup of CA Private Signature Key

CA private signature keys shall be backed up under multi-person control, as specified in Section 0.

A copy of the CA private signature key shall be stored at or near the CA location and off site.

Procedures for Key Backup shall be defined in the applicable CPS.

All copies of the CA private signature key shall be accounted for and protected in the same manner as the original.

6.2.1.3 Backup of Subscriber Private Signature key

At the *MediumHardware* Assurance Levels, Subscriber private signature and identity private keys shall not be backed up or copied.

At the Medium Assurance Level (software key storage per Section 6.1.1), Subscriber private signature keys may be backed up or copied but shall be held in the Subscriber's control. Backed up Subscriber private signature keys shall not be stored in plain text form outside the Cryptographic Module. Storage shall ensure security controls consistent with the protection provided by the Subscriber's Cryptographic Module.

6.2.1.4 Backup of CSA Subscriber Key Management Private Keys

Backed up Subscriber Key Management Keys shall not be stored in plain text form outside the Cryptographic Module. Storage shall ensure security controls consistent with the protection provided by the Subscriber's Cryptographic Module.

A single Backup copy of the CSA private signature key may be stored at or near the CSA location. A second Backup copy may be kept at the CSA Backup location. Procedures for CSA private signature key Backup shall be included in the appropriate CPS.

6.2.1.5 Backup of CSA Private Key

CSA Private Keys may be backed up. If backed up, all copies shall be accounted for and protected in the same manner as the original.

6.2.1.6 Backup of High-ContentSigning Key

No Stipulation.

6.2.1.7 Backup of NPE Private Keys

NPE Private Keys may be backed up or copied but shall be held under the control of the Device Sponsor or other authorized administrator. Backed up NPE Private Keys shall not be stored in plaintext form outside the Cryptographic Module. Storage shall ensure security controls consistent with the protection provided by the NPE's Cryptographic Module.

Private Key Archival

Private signature keys shall not be archived.

Private Key Transfer into or from a Cryptographic Module

CA, and CSA Private Keys may be exported from the Cryptographic Module in accordance with Key Backup procedures as described in Section 0.

At no time shall a CA or CSA Private Key exist in plain text outside the Cryptographic Module.

Private or symmetric keys used to encrypt other Private Keys for transport shall be protected from disclosure.

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 an authentication mechanism that is in compliance with the FIPS 140-2 rating of the Cryptographic Module. The Cryptographic Module storing the key shall be at least as strong as that required in Section 0.

Method of Activating Private Keys

The user shall 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. When pass-phrases or PINs are used, they shall be a minimum of six (6) characters. Entry of Activation Data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

Methods of Deactivating Private Keys

Cryptographic Modules that have been activated shall not be 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.

When Private Keys are deactivated, they shall be cleared from memory before the memory is de-allocated. Any disk space where Private Keys were stored shall be overwritten before the space is released to the operating system.

CA and CSA Hardware Cryptographic Modules shall be removed and stored in a secure container when not in use.

Method of Destroying Private Keys

Private signature keys shall be destroyed when they are no longer needed or when the Certificates to which they correspond expire or are revoked. For software Cryptographic Modules, this can be accomplished by overwriting the data. For hardware Cryptographic Modules, this shall likely be accomplished by executing a “zeroize” command. For CA, RA and CSA private signature keys, the keys shall be destroyed by individuals in Trusted Roles.

The subscriber shall be responsible for private key destruction for device certificates under their control.

At the end of the key pair lifecycle, the subscriber's private key, including all copies and key fragments, shall be securely destroyed to ensure that it is irrecoverable.

Physical destruction of hardware is not generally required.

Practice Note: *For systems like Thales HSMs that do not use key fragments, the entire private key and associated backups are securely destroyed.*

Cryptographic Module Rating

See Section 0.

6.3 OTHER ASPECTS OF KEY MANAGEMENT

Public Key Archival

The Public Key is archived as part of the Certificate archival.

Certificate Operational Periods/Key Usage Periods

See Section 5.6

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 shall 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 lifetimes for Certificates and associated Private Keys.

Key	RSA 2048 Bits / ECC P-224 Bits		RSA 3072 Bits / ECC P-256 Bits		RSA 4096 Bit / ECC P-384 Bits	
	Private Key	Certificate	Private Key	Certificate	Private Key	Certificate
Root CA	20 years	20 years	20 years	20 years	20 years	20 years
Bridge or Issuing CA	10 years	13 years	10 years	13 years	10 years	13 years
Cross Certificates	3 years	≤ 3 years	3 years	≤ 3 years	3 years	≤ 3 years
NPE Identity	3 years	≤ 3 years	3 years	≤ 3 years	3 years	≤ 3 years
Ground NPE Identity for ATN/IPS	3 years	≤ 3 years	3 years	≤ 3 years	3 years	≤ 3 years
NPE Signature	3 years	≤ 3 years	3 years	≤ 3 years	3 years	≤ 3 years
NPE Encryption	n/a	≤ 3 years	n/a	≤ 3 years	n/a	≤ 3 years
Aircraft or Aircraft Equipment Identity	3 years	≤ 3 years	3 years	≤ 3 years	3 years	≤ 3 years
Aircraft Identity for ATN/IPS	3 years	≤ 3 years	3 years	≤ 3 years	3 years	≤ 3 years
Aircraft Signature for ATN/IPS	3 years	≤ 3 years	3 years	≤ 3 years	3 years	≤ 3 years
Aircraft Encryption for ATN/IPS	n/a	≤ 3 years	n/a	≤ 3 years	n/a	≤ 3 years
OCSP Responders	3 years	1 month	3 years	1 month	3 years	1 month
Time-stamp Authority	1 year	≤ 20 years	1 year	≤ 20 years	1 year	≤ 20 years

* For purposes of determining key usage lifetime, it shall commence on activation of the Key Pair.

Practice Note: *Maximum lifetimes are also limited to the Duration of acceptance for a cryptographic algorithm.*

A CA shall not generate a Certificate for a Subscriber whose validity period would be longer than the CA Certificate validity period. As a consequence, the CA Key Pair shall be changed at the latest at the time of CA Certificate expiration minus Subscriber Certificate validity Duration.

Notwithstanding the above table, in all cases the CA Private Key may be used to sign OCSP Certificates and CRLs until the CA Certificate expires.

For some applications (e.g., protected aircraft to ground communications), the Device key may be archived by the CA, upon crypto-period expiration and/or key replacement, to support recovery of encrypted messages, as necessary to comply with regulatory requirements regarding data retention (See sections 9.17.5 and 5.5). Such Archives shall be described in the KRP or the combined CP/KRP (see section 4.12.1 Key Escrow and Recovery Policy and Practices) Organizational Code-Signing Certificate, or Role Based Aircraft Code-Signing Keys).

6.3.1.1 Organizational Code-Signing Certificate, or Role Based Aircraft Code-Signing Keys)

For a Code-Signing Certificate issued to a Corporation or Organization as a whole, the Subscribers and/or Subscriber's Employers shall keep a log stating possession of the Private Key, including the name of the individual to whom the Private Key was entrusted, and the time and date it was entrusted to them.

For Role based Code Signing Certificates where the Keys are used to sign Aircraft software parts, the Role sponsor, or the Role Sponsor’s employer shall keep a log stating to whom such Role Certificates were issued.[3]This log shall be kept for a minimum of thirty (30) years, or as further required by Industry Regulation. The Subscriber and/or Subscriber's Employer are responsible to ensure that the individual in possession of the Private Key corresponding to a Certificate of either type complies with this CP. Moreover, log information maintained by the Subscriber and Affiliated Organization may be audited by the CA or RA at any time.

6.4 ACTIVATION DATA

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.

A Subscriber may select its own Activation Data. For CAs, Activation Data shall either be Biometric data or satisfy the policy enforced at/by the Cryptographic Module.

If the Activation Data shall be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated Cryptographic Module.

When a CA uses passwords as Activation Data for the CA signing key, at a minimum the Activation Data shall be changed upon CA re-key.

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 shall be:

- Memorized or

[3] Since the individual is issued a distinct Certificate, tracking the Certificate lifetime is sufficient to know when that Individual had the capability to sign software parts.

- Biometric in nature, or
- recorded and secured at the level of assurance associated with the activation of the Cryptographic Module and shall not be stored with the Cryptographic Module.

The protection mechanisms shall include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts as defined in the applicable CPS.

Other Aspects of Activation Data

CA, CSA and RA shall change Activation Data whenever the Token is re-keyed or returned for maintenance.

6.5 COMPUTER SECURITY CONTROLS

Specific Computer Security Technical Requirements

CA, CSA, STP and RA shall provide the following computer security functionality through operating system, software, and physical safeguards (in a VME, these functions are applicable to both the VM and Hypervisor):

- Require authenticated logins.
- Provide Discretionary Access Control.
- Provide a security audit capability.
- Restrict Access Control to CA services and PKI roles.
- Enforce separation of duties for PKI roles.
- Require identification and authentication of PKI roles and associated identities.
- Prohibit object re-use.
- Require use of cryptography for session communication and database security.
- Require a trusted path for identification and authentication.
- Enforce domain integrity boundaries for security critical processes.
- Support recovery from key or system failure.
- CAs shall have a recovery mechanism for keys and the CA system.

When CA equipment is hosted on evaluated platforms in support of computer security assurance requirements then the system (e.g., 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.

CA equipment shall be configured with a minimum of the required accounts, and network services.

The Root CAs shall be operated offline with no network connections installed.

The computer system hosting the CA, CSA and STP shall have been hardened against all known Threats. The OA shall conduct an information security safety risk analysis in accordance with section 2.3.3.2 of ICAO Doc 10204 or based on a process approved by the Entity PMA.

Computer Security Rating

No stipulation.

6.6 LIFE-CYCLE (TECHNICAL) SECURITY CONTROLS

System Development Controls

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

- For commercial off-the-shelf software, the software shall be designed and developed under a formal, documented development methodology.
- Where open-source software has been utilized, the CA shall demonstrate that security requirements were achieved through software verification and validation and structured development/lifecycle management.
- Procured hardware and software shall be purchased and shipped in a fashion to reduce the likelihood that any component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).
- Custom developed hardware and software shall be developed in a controlled environment and the development process shall be defined and documented.
- Hardware (e.g., HSM, Computers, and Firewalls) shall be shipped or delivered via controlled methods that provide a continuous chain of accountability from the purchase location to the operations location.
- The hardware and software, including the VME Hypervisor, shall be dedicated to operating and supporting the CA (e.g., the system and services dedicated to the issuance and management of Certificates). There shall be no other applications; hardware devices, network connections, or component software installed which is not part of the PKI operation. In a VME, a single Hypervisor may support multiple CAs and their supporting systems, provided all systems have comparable security controls and are dedicated to the support of the CA.
- In a VME, all VM systems shall operate in the same security zone as the CA.
- Proper care shall be taken to prevent malicious software from being loaded onto the equipment. Software required to perform PKI operations shall be obtained from authorized sources. 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.

The System Development Controls for RA are as follows:

- Hardware and software shall be scanned for malicious code on first use and periodically thereafter.

Security Management Controls

The configuration of the CA, CSA equipment as well as any modifications and upgrades shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the CA, and CSA software or configuration. For CAs operating at medium Level of assurance and above, a formal configuration management methodology shall be used for installation and ongoing maintenance of the CA, and CSA equipment. 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.

Life Cycle Security Ratings

The CPS for each CA shall document how the equipment (hardware and software) used for the PKI is procured, installed and maintained.

6.7 NETWORK SECURITY CONTROLS

Root CAs and their internal PKI repositories shall be offline.

Online CAs, CSAs, RAs, remote workstations used to administer the CAs, and directories containing CA and CRL publications (or distribution) points shall employ appropriate security controls to protect against denial of service and intrusion. Such measures shall include the use of guards, Firewalls, and filtering routers. Networking equipment shall turn off unused network ports and services. Any network software present shall be necessary to PKI operations.

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.

RA equipment shall, at a minimum, be protected by a local Firewall and malware protection. Additionally, all access by the RA equipment to the CA shall be via a protected and mutually authenticated channel using cryptography commensurate with the level of the credentials being managed by that RA.

6.8 TIME STAMPING

All CA, and CSA equipment shall regularly (within 3 minutes) synchronize with a time service such as the National Institute of Standards and Technology (NIST) Atomic Clock or the NIST Network Time Protocol (NTP) service.

Time derived from this time service shall be used for establishment of the following times:

- Initial validity time of a Subscriber's Certificate
- Revocation of a Subscriber's Certificate
- Posting of CRL Updates and CRL validity time
- OCSP or other CSA responses
- Audit Log Timestamps

Asserted times shall be accurate to within three minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events, (see Section 0)

A CA may, at its discretion, offer a Time-Stamp Authority service as defined in RFC 3161.

7. CERTIFICATE, CRL AND OSCP

7.1 CERTIFICATE PROFILE

Version Numbers

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

Certificate Extensions

Critical private extensions shall be interoperable in their intended community of use (which may be a Domain or Region or other community of use).

Issuer CA and Subscriber Certificates may include any extensions as specified by RFC 5280 in a Certificate, but shall include those extensions required by this CP. Any optional or additional extensions shall be non-critical and shall not conflict with the Certificate and CRL profiles defined in this CP. Section 10 contains the Certificate formats.

Interoperability testing shall be completed by testing a representative set of end user applications for successful Certificate usage. Algorithm Object Identifiers

Certificates issued by CAs shall identify the signature algorithm using one of the following OIDs:

SHA256WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
Sha384WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12 }
Sha512WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13}
ecdsa-with-SHA224	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 1 }
ecdsa-with-SHA256	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2 }
ecdsa-with-SHA384	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 3 }
id-Ed448	{ id-edwards-curve-algs 113 } with id-edwards-curve-algs OBJECT IDENTIFIER ::= { 1 3 101 }
Id-Ed25519	{ id-edwards-curve-algs 112 } with id-edwards-curve-algs OBJECT IDENTIFIER ::= { 1 3 101 }

All SHA algorithms above are taken from the SHA-2 family.

Certificates issued by CAs shall identify the cryptographic algorithm associated with the Subject Public Key using one of the following OIDs:

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) id-publicKeyType(2) 1 }

Name Forms

The subject and issuer fields of the Certificate shall be populated with an X.500 Distinguished Name. Distinguished names shall be composed of standard attribute types found in RFC 5280. Certificates issued for use as ETSI-qualified certificates shall use name form option 1.

7.1.1.1 Name Forms for FAA CAs

Subject Name Form for CAs				
OPTION	**USAGE**	**ATTRIBUTE**	**REQUIRED COUNT**	**CONTENT**
1	Required	CN	0..1	Descriptive name for CA, e.g., "CN=XYZ Inc CA"
	Optional	OU	0..N	As needed
	Required	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"
	Optional	DC	1	Domain name, e.g., "DC=xyzinc"
	Optional	DC	1..N	Domain root label(s), e.g., "DC=com" or "DC=com, DC=au", etc.

Subject Name Form for CAs				
OPTION	**USAGE**	**ATTRIBUTE**	**REQUIRED COUNT**	**CONTENT**
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.

7.1.1.2 Name Forms for Organizations

Subject Name Form for Organizations				
OPTION	**USAGE**	**ATTRIBUTE**	**REQUIRED COUNT**	**CONTENT**
1	Recommended	CN	0…1	Descriptive name for organization, e.g., “CN=ABC Inc”
	Optional	OU	0…N	As needed
	Recommended	OU	0…1	“Corporations”, “Organizations”, or similar text
	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)

Subject Name Form for Organizations

OPTION	USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
2	Recommended	CN	0…1	Descriptive name for organization, e.g., “CN=ABC Inc”
	Optional	OU	0…N	As needed
	Recommended	OU	0…1	“Corporations”, “Organizations”, or similar text
	Optional	O	0…1	Issuer name, e.g., “O=XYZ Inc” exactly as it appears in the CA Certificate(s)
	Required	DC	1	Domain name, e.g., “DC=xyzinc” exactly as it appears in the CA Certificate(s)
	Required	DC	1…N	Domain root label(s), e.g., “DC=com” or, “DC=com, DC=au”, etc. exactly as it appears in the CA Certificate(s)

7.1.1.3 Name Forms for Other Entities

Subject Name Form for Other Entities

OPTION	USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
1	Required	See Content column cell to the 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 Content column cell to the 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)
	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 (RDN).

Practice Note: *An example is if the OU is both IT Department and Technical Departments, do not use OU=IT/technical department but instead use OU=IT, OU=Technical Department.*

Aircraft Identifications shall be identifiers registered in an aerospace industry-recognized registry and verifiable by the CA (e.g., serial number, airframe, aircraft or engine registration).Name Constraints

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

In circumstances where the Entity CA does not assert name constraints, Entity CA shall disclose to the other Entity CA to which it cross certifies the name space appropriate for their domains and evidence that such domains are in fact appropriate. The CAs shall not obscure a Subscriber Subject name. Issuer names shall not be obscured.

Name Constraints

In the case where a CA certifies another CA within the PKI, the certifying CA imposes restrictions on the namespace authorized in the Subordinate CA, which are at least as restrictive as its own name constraints.

The CAs do not obscure the Subscriber Subject name. Issuer names are not obscured. Those options are not available in the Certificate Request Form.

Certificate Policy Object Identifier

Except for Self-Signed Root CA, all CA and Subscriber Certificates issued under this CP shall assert one or more of the Certificate policy OIDs listed in Section 1.2 .2. Unless otherwise specified in a Certificate Profile in Section 10, when a CA asserts a policy OID, it shall also assert all policy OIDs corresponding to the lower Assurance Levels defined in this CP.

The following restrictions apply to the aforementioned requirements:

- Organizational Code-Signing Certificates shall only include the Organizational Medium Hardware Code-Signing OID, and none of the other OIDs defined in this CP. This is for legacy purposes only.
- Role Based Code-Signing Certificates used for Aircraft Code Signing shall assert at least the medium-hardware policy OIDs.

A CA issuing subscriber certificates containing its own arc policy OIDs should include policy OIDS from this CP..

Usage of Policy Constraints Extension

Certificates issued by the CA shall assert the policy constraints extensions to inhibit policy mapping.

CAs may assert policy constraints in CA Certificates only where specifically allowed in the Certificate Profiles in this CP (see Section 10. to ensure interoperability).

For Subordinate CA Certificates *inhibitPolicyMappings*, skipCcerts shall be set to 0.

Policy Qualifiers Syntax and Semantics

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

Processing Semantics for the Critical Certificate Policy Extension

Processing semantics for the critical Certificate Policy extension shall conform to X.509 and RFC 5280 certification path processing rules.

7.2 CRL PROFILE

Version Numbers

CAs shall issue X.509 version two (v2) CRLs (populate version field with integrate value of ‘1’).

CRL Entry Extensions

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

Section 10 contains the CRL profiles.

7.3 OCSP PROFILE

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

Version Number

The version number for request and responses shall be v1.

OCSP Extensions

Responses shall support the nonce extension.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

CAs shall have a compliance audit mechanism in place to ensure that the requirements of this CP, their CP and CPS and the provisions of the contracts with cross-certified CAs are being implemented and enforced.

CAs shall be responsible for ensuring Audits are conducted for all PKI functions regardless of how or by whom the PKI components are managed and operated.

By issuing Certificates under this CP, CAs state to Relying Parties that their practices fully comply with this CP.

It is strictly prohibited for any person or organization to falsely claim compliance with this CP, and such claims may give rise to legal actions against persons or Entities disregarding this prohibition.

CAs shall ensure Internal Security assessments are conducted on the PKI infrastructure as required by Agency policy.

8.1 FREQUENCY OF AUDIT OR ASSESSMENTS

All CAs, CSAs and RAs shall be subject to a periodic Compliance Audit, and such Audits shall be conducted on both a scheduled and impromptu basis and shall take place at least once per year.

8.2 IDENTITY AND QUALIFICATIONS OF ASSESSOR

The compliance auditor, whether sourced from an external independent firm or internally, shall:

- have qualifications in accordance with the best commercial practice and as mandated by law or appropriate regulatory agency or board.
- be a certified ISO/IEC27001 lead auditor **(e.g. PECB or equivalent)** or a Certified Information Systems Auditor (CISA).
- have a Certified Information Systems Security Professional (CISSP) qualification.
- have minimum of 5 years of working experience with PKI technology.
- demonstrate competence in the field of Compliance Audits. .
- at the time of the Audit, be thoroughly familiar with the requirements of the applicable [this] CP[s] and the CA's CPS.
- perform such Compliance Audits as a primary responsibility.
- perform Compliance [CA or Information System Security] Audits as a regular ongoing business activity [its primary responsibility].

The applicable CPS should identify the compliance auditor and justify its required qualifications.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

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

In the event the organization chooses to engage compliance auditor services (PKI audits) internal to its parent organization, it shall undergo an Audit from an external third-party audit firm no less often than every third year.

If an external auditor reports any discrepancies in its findings, the entity shall not use its internal auditor services again until an external audit of the entity shows no findings for at least two consecutive years.

8.4 TOPICS COVERED BY ASSESSMENT

The purpose of a Compliance Audit of a PKI shall be to verify that the FAA is complying with the requirements of the applicable CP, and CPS, and any other applicable agreement that governs the FAA PKI. The Compliance Audit shall also include a compliance analysis assessment that determines whether the applicable CPS adequately addresses and implements the requirements of the applicable CP.

If the auditor uses statistical sampling, all PKI components, PKI component managers and operators shall be considered in the sample. The samples shall vary on an annual basis.

Practice Note: *The self-audit sample is a 3% sample of the lifecycle management of the digital certificates. The assessment validates compliance with policies and procedures as defined by the CP, CPS and related procedures. Furthermore, the assessment focusses on the training records of trusted roles and trusted agents to verify that they meet the standards required to authorize certificate issuance.*

For certificate profile compliance, utilize tools like the Lint tool to automatically verify that issued certificates are conformant to the certificate policy (CP) and naming forms, allowing for the efficient processing of large volumes of certificates. Manually inspect only those certificates that fail automated checks, focusing resources on potential non-compliances.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

For the Entity CAs, 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 applicable CPS or any cross-certification or other applicable agreements, the following actions shall be performed:

- The compliance auditor shall document the discrepancy and provide a copy to the OA and PMA Chair.
- The PMA Chair shall provide a copy of the discrepancy documentation to the PMA and schedule a PMA meeting for the OA to report the findings and planned corrective action to the PMA.
- The PMA will determine what further notifications or actions are necessary to meet the requirements of this CP and any agreements and will 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 PMA may direct the OA to take additional actions as appropriate, including temporarily halting operation of the CA.

PMA Notification

Any discrepancy between the CA's operation and a stipulation of its CPs/CPS shall be noted as a deficiency and all direct trust CAs notified immediately. A remedy shall be determined according to Section 8.5.2 and all direct trust CAs shall be notified as to the time for completion.

Remedy

The PMA may determine that a CA is not complying with its obligations set forth in this CP or any agreement pertaining to cross-certified PKIs.

When such a determination is made, the PMA may suspend operation, may revoke the CA, or take other actions as appropriate. The respective CPS shall provide the appropriate procedures.

When the compliance auditor finds a discrepancy between how the CA is designed or is being operated or maintained, and the requirements of this CP or any agreement with cross-certified PKIs, or the applicable CPS, the following actions shall be performed:

- The compliance auditor shall note the discrepancy.
- The compliance auditor shall notify the PMA of the discrepancy.
- The PMA shall notify any affected cross-certified external PKI domains' PMAs 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 respective contracts, and then proceed to make such notifications and take such actions without delay.
- The PMA shall notify any affected cross-certified external PKI domains' PMAs 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 respective contracts, 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 PMA may decide to halt temporarily operation of the CA, to Revoke a Certificate issued by the CA, or take other actions it deems appropriate. The PMA shall develop procedures for making and implementing such determinations.

Remedy by other CAs

Any remedy may include that other cross-certifying CAs may:

- immediately revoke Cross-Certification Certificates of the CA, or
- allow the deficient CA to continue operation for ninety (90) days pending correction of any problems prior to Revocation, or
- indicate the irregularities but allow the deficient CA to continue operations until the next Audit without Revocation.

Factors Considered

The decision regarding what actions to take shall be based on previous responses to problems, the severity of the deficiency, the Risks a prohibition may impose and the disruption to the Community, and the recommendations of the Auditor.

Cross-Certification

If a Cross-Certificate of another CA is revoked, the CA shall immediately update the ARL once notification of such Revocation is received. The CA shall notify all of its Subscribers and Affiliated Organizations and indicate how it will proceed.

8.6 COMMUNICATIONS OF RESULTS

On an annual basis, the OA shall submit the CA compliance audit package to the PMA for review. This package shall be prepared in accordance with the “Compliance Audit Requirements” document and shall include an assertion from the OA that all PKI components have been audited - including any components that may be separately managed and operated. The package shall identify the versions of the CP and CPS used in the assessment.

For CA cross-certifications established with another Bridge, the PMA shall submit the compliance audit package to that Bridge’s Management Authority in compliance with the relevant cross-certification agreement.

Additionally, where necessary, the results shall be communicated as set forth in Section 8.5 above.

Practice Note: *Components of the PKI may be audited separately. In such cases, the compliance audit package may include multiple audit reports (e.g., one per component) or the audit results may be aggregated by the CA compliance auditor.*

Persons to be Notified

Conclusive results of the audits shall be distributed to the RA, the CA, and all Cross-Certified CAs. “Conclusive results” is here defined to be the information of all deficiencies that may affect a Relying Party’s trust in a Certificate, including without limitation an adequate judgment of its level of seriousness but excluding detailed information that can be used to attack the system.

Communication of Remedy

The auditor shall notify any CA or RA found not in compliance with this CP within 5 business days after the completion of the audit. To further mitigate Risk, the auditor shall include in the notice possible remedies and implementation schedules to such CA or RA. The auditor shall communicate the needed implementation of remedies to the CA Operator. If necessary, the auditor or Cross-Certifying CAs shall conduct a special audit to confirm the implementation and effectiveness of the remedy.

Retention of Audit Report

Results of all Audits, as well as the data used to generate these results shall be kept for a minimum of ten and a half years as stipulated in Section 5.5.1 or as further required by applicable law or industry regulation.

Self-Audits

The Issuer CA shall perform regular internal Audits of its operations, personnel, and compliance with this CP using a randomly selected sample of Certificates issued since the last internal Audit. The Issuer CA shall self-audit at least three percent of all Certificates.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

Certificate Issuance/Renewal Fees

No Stipulation.

Certificate Access Fees

No Stipulation.

Revocation or Status Information Access Fee

No Stipulation.

Fees for other Services

No Stipulation.

Refund Policy

No Stipulation.

9.2 FINANCIAL RESPONSIBILITY

Insurance Coverage

FAA CAs that need to contract or cross certify with Non-governmental Entities who are CAs, CMSs, CSSs, or RAs shall ensure that the Non-governmental Entity maintain reasonable levels of insurance coverage to address all foreseeable liability obligations to the FAA and other entities participating in the FAA PKI.

Other Assets

FAA CAs that need to contract or cross certify with Non-governmental Entities who are CAs, CMSs, CSSs, or RAs shall ensure that the Non-governmental Entity maintain sufficient financial resources to maintain operations and fulfill their obligations.

Insurance/warranty Coverage for End-Entities

FAA CAs that need to contract or cross certify with Non-governmental Entities who are CAs, CMSs, CSSs, or RAs shall ensure that the Non-governmental Entity maintain sufficient financial resources to maintain operations and fulfill their obligations.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

No Stipulation.

Information Not Within the Scope of Confidential Information

No Stipulation.

Responsibility to Protect Confidential Information)

No Stipulation.

9.4 PRIVACY OF PERSONAL INFORMATION

Privacy Plan

Consistent with applicable law and FAA Order 1370.121B and FAA Information Security and Privacy: Governance Supplemental Implementation Directive Table 18, the Parties shall have a current Privacy Plan and Policy. All personnel who receive or collect Personally Identifiable Information ("PII") or Personal Information ("PI") (collectively, "PII/PI") while operating the PKI or working in the PKI environment shall be trained on the Privacy Plan and Policy. 3.1.b.(5) The CAs, CMSs, and RAs that collect, store, process, or disclose PII/PI shall adhere to the written Privacy Plan and Policy that is readily available to Subscribers and subject to applicable law and 1370.121B. Information treated as Private

Information treated as Private

As provided in FAA Information Security and Privacy: FAA Implementation of NIST Controls Appendix 14.1, Personally Identifiable Information (PII) is information that can be used to distinguish or trace an individual's identity such as the individual's name, Social Security Number (SSN), biometric records, etc., alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. Such information is covered by the Privacy Act and shall be treated as private, and the FAA must determine and document the legal authority that permits the collection, use, maintenance, and sharing of PII, either general or in support of a specific program or system need. Appendix 14.2. The collected PII must only be used for purposes compatible with the original purpose for which it was collected. Appendix 14.1. Such information shall only be disclosed with the prior written consent of the individual to whom the PII pertains, except as provided by law. Appendix 14.4.b.

Information not deemed Private

As allowed by applicable law, PII included in certificates will not be considered private or subject to protections as outlined in this section. As the use of the information in Certificates is key to the successful operation of the PKI, Subscribers shall be advised that information contained in their certificates shall not be considered private. Certificates shall not be issued if a potential Subscriber does not agree that certificate information is not considered private. See section 9.6.3.

Responsibility to Protect Private Information

See Section 9.4.2.

Notice and Consent to use Private Information

Normally, PII shall only be disclosed with the prior written consent of the individual to whom the PII pertains. See 9.4.6 below for exceptions. CAs, CMSs, and RAs are not required to provide any notice or obtain the consent of the Subscriber or Entity personnel if the Subscriber or Entity personnel have agreed per section 9.6.3 that the information in their Certificate is not private and the use is consistent with the operation of the PKI. Subscriber or Entity may provide notice that they are withdrawing their consent for release. In that event, the CA may revoke their Certificate(s).

Disclosure Pursuant to Judicial/Administrative Process

As allowed by applicable law and provided by FAA Information Security and Privacy: FAA Implementation of NIST Controls Appendix 14, PII shall only be disclosed with the prior written consent of the individual to whom the PII pertains, unless the disclosure would be consistent with the exceptions listed in section 4.b. of the Appendix, which includes release mandated by a court order and other uses consistent with law.

Other Information Disclosure Circumstances

No Stipulation.

9.5 INTELLECTUAL PROPERTY RIGHTS

FAA CAs that need to cross certify with Entities who are CAs shall ensure that no cross-certifying Entity will claim ownership of any pre-existing or independently developed intellectual property of the other Entities or the FAA, including any pre-existing or independently developed software, systems, tools, utilities, processes, technologies, algorithms, know-how, techniques, methods of doing business, policies, practice statements, certificates or attributes issued by or for the other Party, revocation information, key pairs, and other Confidential Information disclosed to the one Entity by another Entity or the FAA.

FAA CAs shall ensure that cross certifying Entities grant the FAA and its contractors providing services to the FAA, a non-exclusive, revocable license to use the Entity Materials provided as may be reasonably necessary to successfully maintain the Cross-Certificates.

Property Rights in Certificates and Revocation Information

FAA CAs shall ensure that Cross-certified Entities include a statement concerning property rights retained by others in its CP with content as follows: Certificate applicants retain all rights to their names (e.g., trademarks, corporate name, and personal name). The subject of a certificate (Subscriber) retains the rights and intellectual property associated with the corresponding private key. FAA and Cross-certified Entities retain ownership of the certificates they issue and the revocation information that they publish.

Property Rights in the CPS

The FAA and cross-certified Entities retain all rights and intellectual property associated with their respective CPSs.

Property Rights in Names

No Stipulation.

Property Rights in Keys

No Stipulation.

9.6 REPRESENTATIONS AND WARRANTIES

No Stipulation.

CA Representations and Warranties

The FAA represents and warrants that to its knowledge:

- All CA signing keys which pertain to unrevoked Certificates are protected, have never been compromised, and are being maintained in a manner consistent with the CP.
- The FAA's Subscribers, if any, have been obligated to a Subscriber Agreement which includes Subscriber representation and warrants. Further, the Subscriber Agreement includes a representation and warranty from the Subscriber that the information 1) they have provided to the CA and 2) in their Certificate is true and accurate.
- The FAA has an Agreement with all Affiliated Organizations for which it presently has unrevoked Certificates. The Agreement incorporates the applicable obligations from this CP and assigns them to the Affiliated Organization.
- The unrevoked Certificates issued by the FAA are being used for authorized and legal purposes.
- The PKI Repository, CRL, and Certificate Status Services (e.g., OCSP) are being maintained in a manner consistent with the CP.

9.6.1.1 Subordinate or Cross-Certified CAs

No Stipulation.

9.6.1.2 Device Sponsor Representations and Warranties

If the Device Sponsor for an NPE is not physically located near the sponsored NPE, and/or does not have sufficient administrative privileges on the sponsored NPE to protect the NPE's Private Key and ensure that the NPE Certificate is only used for authorized purposes, the Device Sponsor may delegate these responsibilities to an authorized administrator for the NPE. The delegation shall be documented and signed by both the Device Sponsor and the authorized administrator for the NPE.

RA Representations and Warranties

No Stipulation.

Subscriber Representations and Warranties

Subscriber shall be required to sign a Subscriber Agreement containing the requirements the Subscriber shall meet respecting protection of the Private Key and use of the Certificate before being issued the Certificate. Specifically, the Subscriber Agreement shall obligate the Subscriber to the following:

- Accurately represent themselves in all communications with the PKI authorities.
- The identity and affiliation information in the Subscriber's Certificate is accurate.
- The Subscriber is the sole user of the key corresponding to Subscriber's Certificate(s) except in key recovery scenarios.
- Protect their Private Keys at all times, in accordance with this Policy, as stipulated in their Certificate acceptance agreements and local procedures.

- 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 the Issuing CA's CPS.
- Abide by all the terms, conditions, and restrictions levied on the use of their Private Keys and Certificates.
- Acknowledge that any information contained within a Certificate is not considered private.

A Device Sponsor shall assume the Subscriber obligations for NPEs.

Relying Parties Representations and Warranties

No Stipulation.

Representations and Warranties of Affiliated Organizations

9.6.1.3 Affiliated Organizations

Affiliated Organizations shall verify and authorize the affiliation of Subscribers with that Organization and shall inform the CA of any severance of affiliation with any current Subscriber by requesting Revocation of the Certificates issued to that Subscriber.

9.7 DISCLAIMERS OF WARRANTIES

No Stipulation.

9.8 LIMITATIONS OF LIABILITY

No Stipulation.

9.9 INDEMNITIES

Indemnification by Entity CA

No Stipulation.

Indemnification by Relying Party

No Stipulation.

Indemnification by Subscribers

No Stipulation.

9.10 TERM AND TERMINATION

Term

This CP has no specified term.

No Stipulation.

Termination

No Stipulation.

Effect of Termination and Survival

The following requirements of this CP remain in effect through the end of the archive period for the last Certificate issued: 2.1.1, 2.2, 5.4, 5.5, 6.2-6.4, 6.8, 9.2-9.4, 9.7-9.10, and 9.13-16.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

No Stipulation.

9.12 AMENDMENTS

Procedure for Amendment

The PMA shall review this CP at least once every year.

Corrections, updates, or suggested changes to this CP shall be communicated to every CA.

This CP and amendments to it shall become effective once approved by the PMA, by the OA, and published into the PKI Repository.

The Specification administrators will endeavor to only use and reference publicly available standards.

For SCAs and cross-certified CAs, they shall follow similar requirements and shall review their CPs for changes at least once per year.

Notification Mechanism and Period

For the CA, proposed changes to this CP shall be distributed electronically to PMA members and observers in accordance with the PMA Charter. The CP approved by the PMA and OA shall be published into the PKI Repository.

For SCAs and cross-certifying CA similar mechanism shall be used.

Circumstances under which OID must be changed

The CA shall change OIDs if the PMA determines that a change in the CP reduces the level of assurance provided.

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

9.13 DISPUTE RESOLUTION PROVISIONS

No Stipulation.

Disputes among the PMA/OA and Third Parties

No Stipulation.

Alternate Dispute Resolution Provisions

No Stipulation.

9.14 GOVERNING LAW

This CP and any Cross-Certification Agreement will be interpreted and governed by the federal law of the United States. The construction, validity, performance, and effect of certificates issued under the FAA NPE CP and Entity CP shall be governed by the federal law of the United States.

9.15 COMPLIANCE WITH APPLICABLE LAW

FAA and Entity CAs shall comply with all applicable laws.

9.16 MISCELLANEOUS PROVISIONS

Entire agreement

No Stipulation.

Assignment

No Stipulation.

Severability

No Stipulation.

Enforcement (Attorney Fees/Waiver of Rights)

No Stipulation.

Force Majeure

No Stipulation.

9.17 OTHER PROVISIONS

Prohibited Certificate Uses

FAA shall not use any Certificate for a prohibited purpose. Prohibited applications are as follows:

- any export, import, use or activity that contravenes any local or U.S. Federal laws or regulations,
- any usage of the Certificates for personal purposes,
- any usage of Certificates in conjunction with illegal activities; and
- any use of a Certificate after it has been suspended or revoked.

Corporate Controls

No Stipulation.

Background, Qualifications, Experience, & Clearance Requirements

No Stipulation.

Background Check Procedures Adjudication

No Stipulation.

Retention Period for Archive

At a minimum, the archive data and the applications required to process it shall be retained for the longer of 10 years and 6 months and the applicable record retention laws in the CAs jurisdiction. Where the retention period is longer than 10 years and 6 months, the applicable CP or CPS shall state the retention period.

If the original media cannot retain the data for the required period, a mechanism to transfer the archived data to new media shall be defined by the archive site. Alternatively, the FAA may retain data using whatever procedures have been approved by the U.S. National Archives and Records Administration or by the respective records retention policies in accordance with whatever laws apply to those entities for that category of documents.

10. CERTIFICATE, CRL AND OCSP PROFILES

10.1 SELF-SIGNED ROOT CERTIFICATE

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

Issuer Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Issuer Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Validity Period	Expressed in UTC Time until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Subject Public Key Information	2048 bit RSA key modulus or greater, rsaEncryption {1 2 840 113549 1 1 1} for ECC: 256 bit prime, 233 bit binary, id-ecPublicKey {1 2 840 10045 2 1} **Practice Note:** *4096 bit lengths for RSA and 384 bit prime for ECC are increasingly prevalent for offline Root CAs within the community and Relying Parties may need to interoperate with such key lengths.*

Issuer's Signature	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Extension	**Value**
Subject Key Identifier	c=no; Octet String (which is calculated as the SHA-1 hash of the BIT STRING subjectPublicKey, excluding the tag, length, and number of unused bits)
Key Usage	c=yes; keyCertSign, cRLSign, If the subject Public Key may be used for purposes other than Certificate and CRL signing (e.g., signing OCSP responses), then the digitalSignature and/or nonRepudiation bits may be set as well.

Field	Value
Basic Constraints	c=yes; cA=True; path length constraint absent

10.2 SELF-SIGNED ROOT CERTIFICATE FOR ATN/IPS

Practice Note: *Additional extensions may be required by relying parties. For example, certain Gatelink implementations require the CRL-DP extension to be asserted.*

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}
Issuer Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Validity Period	Expressed in UTC Time until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Subject Public Key Information	384 bit prime id-ecPublicKey {1 2 840 10045 2 1} with parameters secp384r1/P-384 {1.3.132.0.34}
Issuer’s Signature	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}
Extension	**Value**
Subject Key Identifier	c=no; Octet String (which is calculated as the SHA-1 hash of the BIT STRING subjectPublicKey, excluding the tag, length, and number of unused bits)
Key Usage	c=yes; keyCertSign, cRLSign,
Basic Constraints	c=yes; cA=True; path length constraint absent

10.3 <ENTITY> SIGNING CA (POLICY CA OR ISSUING CA CERTIFICATE)

Practice Note: *Additional extensions may be required by relying parties. For example, certain Gatelink implementations require the CRL-DP extension to be asserted.*

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

Issuer Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384{1 2 840 10045 4 3 3}

Issuer Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Validity Period	Expressed in UTC Time until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Subject Public Key Information	2048 bit RSA key modulus or greater, rsaEncryption {1 2 840 113549 1 1 1} for ECC: 256 bit prime, 233 bit binary, id-ecPublicKey {1 2 840 10045 1 2} **Practice Note:** 4096 bit lengths for RSA and 384 bit prime for ECC are increasingly prevalent for Policy or Issuing CAs within the community and Relying Parties may need to interoperate with such key lengths.

Issuer's Signature	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA)
Subject Key Identifier	c=no; Octet String (which is calculated as the SHA-1 hash of the BIT STRING subjectPublicKey, excluding the tag, length, and number of unused bits)
Key Usage	c=yes; keyCertSign, cRLSign

Field	Value

Certificate Policies	c=no; {applicable policies}
	{CP Medium-Hardware-Device LoA OID}
	CPS:<URL of the public Accessible CP PDF>
	User Notice: Explicit Test: This certificate has been issued in accordance with the <Entity> PKI Certificate Policy as found in the CPSpointer field

Basic Constraints	c=yes; cA=True; path length constraint absent or as desired by IssuingCA
Name Constraints	c=yes; optional, permitted subtrees for DN, RFC 5322, and DNS name forms
Policy Constraints	c= no; optional
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may contain id-ad-ocsp access method entry with HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no; optional; This extension should appear in all Sub-CA Certificates and must contain at least one HTTP URI. The reasons and cRLIssuer Fields must be omitted.

3115
10.4 <ENTITY> SIGNING CA FOR ATN/IPS

3116

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	ecdsa-with-SHA384{1 2 840 10045 4 3 3}
Issuer Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Validity Period	Expressed in UTC Time until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Subject Public Key Information	ECC 256 bit prime, id-ecPublicKey {1 2 840 10045 1 2} with parameters secp256r1/P-256 (1.2.840.10045.3.1.7)}
Issuer's Signature	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in ATN/IPS Root CA)
Subject Key Identifier	c=no; Octet String (which is calculated as the SHA-1 hash of the BIT STRING subjectPublicKey, excluding the tag, length, and number of unused bits)
Key Usage	c=yes; keyCertSign, cRLSign

Certificate Policies	c=no;
	{CP Medium-Hardware-Device LoA OID} and {CP Medium-Software-Device LOA}
	CPS:<URL of the public Accessible CP PDF>
	User Notice: Explicit Test: This certificate has been issued in accordance with the <Entity> PKI Certificate Policy as found in the CPSpointer field

Field	Value
Basic Constraints	c=yes; cA=True; path length constraint absent or as desired by IssuingCA
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, shall contain id-ad-ocsp access method entry with HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no; optional; This extension shall appear in all Sub-CA Certificates and must contain at least one HTTP URI pointing to a DER encoded complete CRL signed by the Issuing CA. The reasons and cRLIssuer Fields must be omitted.

10.5 DEVICE IDENTITY CERTIFICATE

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

Issuer Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Issuer Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Validity Period	Expressed in UTC Time until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 subject DN conforming to Section 7.1.4 of this CP cn={ Host URL | Host IP Address | Host Name }
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1} for ECC: 256 bit prime, 233 bit binary, id-ecPublicKey {1 2 840 10045 2 1} or greater as specified in Section 6.1.5.

Issuer's Signature	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA)
Subject Key Identifier	c=no; Octet String (which is calculated as the SHA-1 hash of the BIT STRING subjectPublicKey, excluding the tag, length, and number of unused bits)
Key Usage	c=yes; (Mandatory) digitalSignature (Optional) keyEncipherment
Extended Key Usage	c=no; per Section 10.27

Field	Value
Certificate Policies	c=no; {applicable policies} CPS:<URL of the public Accessible CP PDF> User Notice: Explicit Test: This certificate has been issued in accordance with the <Entity> PKI Certificate Policy as found in the CPSpointer field
Subject Alternative Name	c=no; (Mandatory) Host URL | IP Address | Host Name **| UUID | RFC 822 Name** one or more dNSName=additional name where "additional name" is per section 7.1.4 **Practice Note: Host Name may be either a DNS or X.500 Name**
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA,; may contain id-ad-ocsp access method entry with HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no; optional; This extension should appear in all Sub-CA Certificates and must contain at least one HTTP URI. The reasons and cRLIssuer Fields must be omitted.

3122 10.6 GROUND DEVICE IDENTITY CERTIFICATE FOR ATN/IPS

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}
Issuer Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Validity Period	Expressed in UTC Time until 2049 and Generalized Time thereafter with maximum duration of 96 hours
Subject Distinguished Name	Unique X.500 subject DN conforming to Section 7.1.4 of this CP cn={ Host URL | Host IP Address | Host Name }
Subject Public Key Information	ECC: 256 bit prime, id-ecPublicKey {1 2 840 10045 2 1} with parameters: Secp256r1/P-256 {1.2.840.10045.3.1.7}
Issuer's Signature	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA)
Subject Key Identifier	c=no; Octet String (which is calculated as the SHA-1 hash of the BIT STRING subjectPublicKey, excluding the tag, length, and number of unused bits)
Key Usage	c=yes; (Mandatory) digitalSignature (Mandatory) keyAgreement
Extended Key Usage	c=no; per Section 10.27
Certificate Policies	c=no; {CP Medium-Hardware-Device LoA}

Field	Value
Subject Alternative Name	c=no; (Mandatory) Host URL | IP Address | Host Name one or more dNSName=additional name where “additional name” is per section 7.1.4
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA,; shall contain id-ad-ocsp access method entry with HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no; optional; This extension shall appear in all Certificates and must contain at least one HTTP URI pointing to a DER encoded CRL signed by the Issuing CA. The reasons and cRLIssuer Fields must be omitted.

10.7 DEVICE SIGNATURE CERTIFICATE

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

Issuer Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Issuer Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 subject DN conforming to Section 7.1.4 of this CP cn={ Host URL | Host IP Address | Host Name}
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1} for ECC: 256 bit prime, 233 bit binary, id-ecPublicKey {1 2 840 10045 2 1} or greater as specified in Section 6.1.5].

Issuer's Signature	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA)
Subject Key Identifier	c=no; Octet String (which is calculated as the SHA-1 hash of the BIT STRING subjectPublicKey, excluding the tag, length, and number of unused bits)
Key Usage	c=yes; (Mandatory) digitalSignature
Extended Key Usage	c=no; per Section 10.27
Certificate Policies	c=no; {applicable policies}

Field	Value
Subject Alternative Name	c=no; (Mandatory) 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,; may contain id-ad-ocsp access method entry with HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no; optional; This extension should appear in all Sub-CA Certificates and must contain at least one HTTP URI. The reasons and cRLIssuer Fields must be omitted.

10.8 DEVICE ENCRYPTION CERTIFICATE

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

Issuer Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Issuer Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 subject DN conforming to Section 7.1.4 of this CP cn={ Host URL | Host IP Address | Host Name}
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1} for ECC: 256 bit prime, 233 bit binary, id-ecPublicKey {1 2 840 10045 2 1} or greater as specified in Section 6.1.5].

Issuer's Signature	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA)
Subject Key Identifier	c=no; Octet String (which is calculated as the SHA-1 hash of the BIT STRING subjectPublicKey, excluding the tag, length, and number of unused bits)
Key Usage	c=yes; keyEncipherment dataEncipherment
Extended Key Usage	c=no; per Section 10.27
Certificate Policies	c=no; {applicable policies}

Field	Value
Subject Alternative Name	c=no; (Mandatory) 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,; may contain id-ad-ocsp access method entry with HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no; optional; This extension should appear in all Sub-CA Certificates and must contain at least one HTTP URI. The reasons and cRLIssuer Fields must be omitted.

10.9 AIRCRAFT OR AIRCRAFT EQUIPMENT IDENTITY CERTIFICATE

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

Issuer Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Issuer Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 subject DN conforming to Section 7.1.4 of this CP cn={Aircraft Identification | Aircraft Equipment Identification (see 7.1.4) }
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1} for ECC: 256 bit prime, 233 bit binary, id-ecPublicKey {1 2 840 10045 2 1} or greater as specified in Section 6.1.5].

Issuer's Signature	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA)
Subject Key Identifier	c=no; Octet String (which is calculated as the SHA-1 hash of the BIT STRING subjectPublicKey, excluding the tag, length, and number of unused bits)
Key Usage	c=yes; (Mandatory) digitalSignature (Optional) keyEncipherment (for RSA) or keyAgreement (for ECC)
Extended Key Usage	c=no; per Section 10.27

Field	Value
Certificate Policies	c=no; {applicable policies}
Subject Alternative Name	c=no; always present, Aircraft Identification | Aircraft Equipment Identification [see Section 7.1.4
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA,; may contain id-ad-ocsp access method entry with HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no; optional; This extension should appear in all Sub-CA Certificates and must contain at least one HTTP URI. The reasons and cRLIssuer Fields must be omitted.

3135 10.10 AIRCRAFT IDENTITY CERTIFICATE FOR ATN/IPS

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}
Issuer Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter with maximum of 3 year validity
Subject Distinguished Name	Unique X.500 subject DN conforming to Section 7.1.4 of this CP cn={Aircraft Identification | Aircraft Equipment Identification (see 7.1.4) }
Subject Public Key Information	ECC: 256 bit prime, id-ecPublicKey {1 2 840 10045 2 1} with parameter Secp256r1/P-256 {1.2.840.10045.3.1.7}
Issuer's Signature	ecdsa-with-SHA256 {1 2 840 10045 4 3 2}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA)
Subject Key Identifier	c=no; Octet String (which is calculated as the SHA-1 hash of the BIT STRING subjectPublicKey, excluding the tag, length, and number of unused bits)
Key Usage	c=yes; (Mandatory) digitalSignature (Mandatory) keyAgreement
Extended Key Usage	c=no; per Section 10.27
Certificate Policies	c=no; {CP Medium-Hardware-Device LoA} OR {CP Medium-Software-Device LoA}

Field	**Value**
Subject Alternative Name	c=no; always present, Aircraft Identification | Aircraft Equipment Identification (see 7.1.4) RegisteredID containing the ICAO 24bit address of the device
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA,; may contain id-ad-ocsp access method entry with HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no; optional; This extension shall appear in all Certificates and must contain at least one HTTP URI pointing to a DER encoded complete CRL signed by the Issuing CA. The reasons and cRLIssuer Fields must be omitted.

3138 10.11 AIRCRAFT OR AIRCRAFT EQUIPMENT SIGNATURE CERTIFICATE

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

Issuer Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Issuer Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 subject DN conforming to Section 7.1.4 of this CP cn={Aircraft Identification | Aircraft Equipment Identification (see 7.1.4) }
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1} for ECC: 256 bit prime, 233 bit binary, id-ecPublicKey {1 2 840 10045 2 1} or greater as specified in Section 6.1.5].

Issuer's Signature	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA)
Subject Key Identifier	c=no; Octet String (which is calculated as the SHA-1 hash of the BIT STRING subjectPublicKey, excluding the tag, length, and number of unused bits)
Key Usage	c=yes; (Mandatory) digitalSignature (Optional) nonRepudiation
Extended Key Usage	c=no; per Section 10.27
Certificate Policies	c=no; {applicable policies}

Field	Value
Subject Alternative Name	c=no; always present, Aircraft Identification | Aircraft Equipment Identification [see Section 7.1.4
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA,; may contain id-ad-ocsp access method entry with HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no; optional; This extension should appear in all Sub-CA Certificates and must contain at least one HTTP URI. The reasons and cRLIssuer Fields must be omitted.

3141 10.12 AIRCRAFT OR AIRCRAFT EQUIPMENT ENCRYPTION CERTIFICATE

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

Issuer Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Issuer Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 subject DN conforming to Section 7.1.4 of this CP cn={ Aircraft Identification | Aircraft Equipment Identification (see 7.1.4) }
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1} for ECC: 256 bit prime, 233 bit binary, id-ecPublicKey {1 2 840 10045 2 1} or greater as specified in Section 6.1.5].

Issuer's Signature	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA)
Subject Key Identifier	c=no; Octet String (which is calculated as the SHA-1 hash of the BIT STRING subjectPublicKey, excluding the tag, length, and number of unused bits)
Key Usage	c=yes; (Mandatory) keyEncipherment (Optional) dataEncipherment
Extended Key Usage	c=no; per Section 10.27
Certificate Policies	c=no; {applicable policies}

Field	Value
Subject Alternative Name	c=no; (Mandatory) Aircraft Identification | Aircraft Equipment Identification (see 7.1.4)
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA,; may contain id-ad-ocsp access method entry with HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no; optional; This extension should appear in all Sub-CA Certificates and must contain at least one HTTP URI. The reasons and cRLIssuer Fields must be omitted.

10.13 SUBSCRIBER IDENTITY CERTIFICATE

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

Issuer Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Issuer Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1} or ECC: 256 bit prime, 233 bit binary, id-ecPublicKey {1 2 840 10045 2 1} or greater as specified in Section 6.1.5].

Issuer’s Signature	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA)
Subject Key Identifier	c=no; Octet String (which is calculated as the SHA-1 hash of the BIT STRING subjectPublicKey, excluding the tag, length, and number of unused bits)
Key Usage	c=yes; DigitalSignature (Mandatory), nonRepudiation (optional)
Extended Key Usage	c=no; per Section 10.27
Certificate Policies	c=no; {applicable policies}

Field	**Value**
Subject Alternative Name	c=no; (Optional unless asserting High Assurance Level) URI urn:uuid:<128 bit GUID> (Optional) others
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA,; may contain id-ad-ocsp access method entry with HTTP URL for the Issuing CA OCSP Responder unless asserting High Assurance Level, in which case mandatory
CRL Distribution Points	c = no; optional; This extension should appear in all Sub-CA Certificates and must contain at least one HTTP URI. The reasons and cRLIssuer Fields must be omitted.

10.14 SUBSCRIBER SIGNATURE CERTIFICATE

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

Issuer Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Issuer Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1} or ECC: 256 bit prime, 233 bit binary, id-ecPublicKey {1 2 840 10045 2 1} or greater as specified in Section 6.1.5].

Issuer's Signature	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Required Extensions	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA)
Subject Key Identifier	c=no; Octet String (which is calculated as the SHA-1 hash of the BIT STRING subjectPublicKey, excluding the tag, length, and number of unused bits)
Key Usage	c=yes; DigitalSignature, nonrepudiation
Extended Key Usage	c=no; per Section 10.27
Certificate Policies	c=no; {applicable policies}

Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for p7c file containing Certificates issued to Issuing CA,; may contain id-ad-ocsp access method entry with HTTP URL for the Issuing CA OCSP Responder unless asserting High Assurance Level, in which case mandatory
CRL Distribution Points	c = no; optional; This extension should appear in all Sub-CA Certificates and must contain at least one HTTP URI. The reasons and cRLIssuer Fields must be omitted.
Optional Extensions	**Value**
Subject Alternative Name	c=no; Any name types may be present. *** If application (s) using Certificates from this Certificate profile use this extension, then this extension is required with the values specified below: (Mandatory) RFC5322 email address (Optional) URI urn:uuid:<128 bit GUID> (Optional) others

10.15 SUBSCRIBER ENCRYPTION CERTIFICATE

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

Issuer Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Issuer Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1} or ECC: 256 bit prime, 233 bit binary, id-ecPublicKey {1 2 840 10045 2 1} or greater as specified in Section 6.1.5].

Issuer's Signature	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA)
Subject Key Identifier	c=no; Octet String (which is calculated as the SHA-1 hash of the BIT STRING subjectPublicKey, excluding the tag, length, and number of unused bits)
Key Usage	c=yes; (Mandatory) keyEncipherment (Optional) dataEncipherment
Extended Key Usage	c=no; per Section 10.27
Certificate Policies	c=no; {applicable policies}

Field	Value
Subject Alternative Name	c=no; (Mandatory) RFC5322 email address (Optional) URI urn:uuid:<128 bit GUID> (Optional) others
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA,; may contain id-ad-ocsp access method entry with HTTP URL for the Issuing CA OCSP Responder unless asserting High Assurance Level, in which case mandatory
CRL Distribution Points	c = no; optional; This extension should appear in all Sub-CA Certificates and must contain at least one HTTP URI. The reasons and cRLIssuer Fields must be omitted.

Practice Note: *Some applications expect an email address in the Subject Alternative Name field. Not having an email address in the field may cause problems as a result.*

10.16 ROLE SIGNATURE CERTIFICATE

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

Issuer Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Issuer Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 subject DN conforming to Section 7.1.4 of this CP cn={ Aircraft Identification | Aircraft Equipment Identification (see 7.1.4) }
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1} for ECC: 256 bit prime, 233 bit binary, id-ecPublicKey {1 2 840 10045 2 1} or greater as specified in Section 6.1.5].

Issuer's Signature	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA)
Subject Key Identifier	c=no; Octet String (which is calculated as the SHA-1 hash of the BIT STRING subjectPublicKey, excluding the tag, length, and number of unused bits)
Key Usage	c=yes; DigitalSignature, NonRepudiation
Extended Key Usage	c=no; per Section 10.27
Certificate Policies	c=no; {applicable policies}

Field	Value
Subject Alternative Name	c=no; (Mandatory) DN of the person controlling the role signing Private Key (Optional) RFC5322 email address (Optional) others
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA,; may contain id-ad-ocsp access method entry with HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no; optional; This extension should appear in all Sub-CA Certificates and must contain at least one HTTP URI. The reasons and cRLIssuer Fields must be omitted.

3158 ## 10.17 ROLE ENCRYPTION CERTIFICATE

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

Issuer Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Issuer Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 subject DN conforming to Section 7.1.4 of this CP cn={ Aircraft Identification | Aircraft Equipment Identification (see 7.1.4) }
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1} for ECC: 256 bit prime, 233 bit binary, id-ecPublicKey {1 2 840 10045 2 1} or greater as specified in Section 6.1.5].

Issuer's Signature	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA)
Subject Key Identifier	c=no; Octet String (which is calculated as the SHA-1 hash of the BIT STRING subjectPublicKey, excluding the tag, length, and number of unused bits)
Key Usage	c=yes; (Mandatory) keyEncipherment (Optional) dataEncipherment
Extended Key Usage	c=no; per Section 10.27

Field	**Value**
Certificate Policies	c=no; {applicable policies}
Subject Alternative Name	c=no; (Mandatory) RFC5322 email address (Optional) others
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA,; may contain id-ad-ocsp access method entry with HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no; optional; This extension should appear in all Sub-CA Certificates and must contain at least one HTTP URI. The reasons and cRLIssuer Fields must be omitted.

3161 ## 10.18 CODE-SIGNING CERTIFICATE

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

Issuer Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Issuer Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter.
Subject Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1} for ECC: 256 bit prime, 233 bit binary, id-ecPublicKey {1 2 840 10045 2 1} or greater as specified in Section 6.1.5].

Issuer's Signature	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA)
Subject Key Identifier	c=no; Octet String (which is calculated as the SHA-1 hash of the BIT STRING subjectPublicKey, excluding the tag, length, and number of unused bits)
Key Usage	c=yes; (Mandatory) digitalSignature (Optional) nonRepudiation
Extended Key Usage	c=no; per Section 10.27
Certificate Policies	c=no; {applicable policies}

Field	Value
Subject Alternative Name	c=no; DN of the person controlling the code signer Private Key
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA,; may contain id-ad-ocsp access method entry with HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no; optional; This extension should appear in all Sub-CA Certificates and must contain at least one HTTP URI. The reasons and cRLIssuer Fields must be omitted.

10.19 ORGANIZATIONAL CODE-SIGNING CERTIFICATE

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

Issuer Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Issuer Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}for ECC: 256 bit prime, 233 bit binary, id-ecPublicKey {1 2 840 10045 2 1} or greater as specified in Section 6.1.5].

Issuer's Signature	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA)
Subject Key Identifier	c=no; Octet String (which is calculated as the SHA-1 hash of the BIT STRING subjectPublicKey, excluding the tag, length, and number of unused bits)
Key Usage	c=yes; (Mandatory) digitalSignature (Optional) nonRepudiation
Extended Key Usage	c=no; per Section 10.27
Certificate Policies	c=no; {applicable policies}

Field	Value
Subject Alternative Name	Not present
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA,; may contain id-ad-ocsp access method entry with HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no; optional; This extension should appear in all Sub-CA Certificates and must contain at least one HTTP URI. The reasons and cRLIssuer Fields must be omitted.

10.20 HIGH-CARD AUTHENTICATION

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

Issuer Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Issuer Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	sn=<GUID> with applicable DN prefix

Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
	for ECC: 256 bit prime, 233 bit binary, id-ecPublicKey {1

Issuer's Signature	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA)
Subject Key Identifier	c=no; Octet String (which is calculated as the SHA-1 hash of the BIT STRING subjectPublicKey, excluding the tag, length, and number of unused bits)
Key Usage	c=yes; (Mandatory) digitalSignature
Extended Key Usage	c=yes; per Section 10.27
Certificate Policies	c=no; {applicable policies}
Subject Alternative Name	c=no; (Mandatory) URI urn:uuid:<128 bit GUID>

Field	Value
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA,; shall contain id-ad-ocsp access method entry with HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no; optional; This extension should appear in all Sub-CA Certificates and must contain at least one HTTP URI. The reasons and cRLIssuer Fields must be omitted.

3170 ## 10.21 HIGH-CONTENT SIGNER

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

Issuer Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Issuer Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1} for ECC: 256 bit prime, 233 bit binary, id-ecPublicKey {1 2 840 10045 2 1} or greater as specified in Section 6.1.5].

Issuer's Signature	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA)
Subject Key Identifier	c=no; Octet String (which is calculated as the SHA-1 hash of the BIT STRING subjectPublicKey, excluding the tag, length, and number of unused bits)
Key Usage	c=yes; (Mandatory) digitalSignature
Extended Key Usage	c=no; per Section 10.27
Certificate Policies	c=no; {applicable policies}
Subject Alternative Name	optional; c=no;

Field	Value
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA,; shall contain id-ad-ocsp access method entry with HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no; optional; This extension should appear in all Sub-CA Certificates and must contain at least one HTTP URI. The reasons and cRLIssuer Fields must be omitted.

10.22 OCSP RESPONDER CERTIFICATE

The following table contains the OCSP Responder Certificate profile assuming that the same CA using the same key as the Subscriber Certificate issues the OCSP Responder Certificate.

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

Issuer Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Issuer Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 subject DN conforming to Section 7.1.4 of this CP
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1} for ECC: 256 bit prime, 233 bit binary, id-ecPublicKey {1 2 840 10045 2 1} or greater as specified in Section 6.1.5].

Issuer's Signature	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA)
Subject Key Identifier	c=no; Octet String (which is calculated as the SHA-1 hash of the BIT STRING subjectPublicKey, excluding the tag, length, and number of unused bits)
Key Usage	c=yes; (Mandatory) digitalSignature, nonRepudiation
Extended Key Usage	c=yes; per Section 10.23
Certificate Policies	c=no; {applicable policies}

Field	Value
Subject Alternative Name	c=no; 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

10.23 TIME-STAMP AUTHORITY SIGNATURE CERTIFICATE

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

Issuer Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Issuer Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter[4].
Subject Distinguished Name	Unique X.500 subject DN conforming to Section 7.1.4 of this CP cn={ Host URL | Host IP Address | Host
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1} for ECC: 256 bit prime, 233 bit binary, id-ecPublicKey {1 2 840 10045 2 1} or greater as specified in Section 6.1.5].

Issuer's Signature	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA)
Subject Key Identifier	c=no; Octet String (which is calculated as the SHA-1 hash of the BIT STRING subjectPublicKey, excluding the tag, length, and number of unused bits)
Key Usage	c=yes; (Mandatory) digitalSignature
Extended Key Usage	c=no; per Section 10.27

[4] To achieve as long as a validity period as possible, the issuer of a time-stamp authority Certificate should be a Root CA.

Field	**Value**
Certificate Policies	c=no; {applicable policies}
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA,; may contain id-ad-ocsp access method entry with HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no; optional; This extension should appear in all Sub-CA Certificates and must contain at least one HTTP URI. The reasons and cRLIssuer Fields must be omitted.

10.24 FULL CRL PROFILE

Field	**Value**
Version	V2 (1)

Issuer Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Issuer Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
thisUpdate	Expressed in UTC Time for dates until end of 2049 and Generalized Time thereafter
nextUpdate	Expressed in UTC Time for dates until end of 2049 and Generalized Time thereafter
Revoked Certificates list	0 or more 2-tuple of Certificate serial number and revocation date Expressed in UTC Time for dates until end of 2049 and Generalized Time thereafter

Issuer's Signature	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

CRL Extension	**Value**
CRL Number	c=no; monotonically increasing integer
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 unless circumstances were for reasons of key compromise or CA compromise
Hold Instruction	c=no; optional. id-holdinstruction-reject may be present only if reason code is CertificateHold

10.25 OCSP REQUEST FORMAT

Field	Value
Version	V1 (0)
Requester Name	(Mandatory) DN of the requestor
Request List	List of Certificates in accordance with RFC 6960
Request Extension	**Value**
None	None
Request Entry Extension	**Value**
None	None

10.26 OCSP RESPONSE FORMAT

Field	Value
Version	V1 (0)

Issuer Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Issuer's Signature	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
	ecdsa-with-SHA384 {1 2 840 10045 4 3 3}

Response Status	As specified in RFC 6960
Response Type	Id-pkix-ocsp-basic {1 3 6 1 5 5 7 48 1 1}
Responder ID	Octet String (same as subject key identifier in Responder Certificate)
Produced At	Generalized Time

Field	**Value**
List of Responses	Each response shall contain Certificate id, Certificate status, thisUpdate, nextUpdate. The OCSP responder shall use thisUpdate and nextUpdate from the CA CRL. If the Certificate is revoked, the OCSP responder shall provide the revocation time and reason corresponding to that asserted in the CA CRL entry extension.
Request List	List of Certificates in accordance with RFC 6960
Request Extension	**Value**
Nonce	c=no; Same value as asserted in the request if it was present in the request
Response Entry Extension	**Value**
None	None

3188

10.27 EXTENDED KEY USAGE

Certificate Type	Required EKU	Optional EKU	Prohibited EKU
CA	None	None	All
OCSP Responder	id-kp-OCSPSigning {1 3 6 1 5 5 7 3 9}	None	All Others
Human Subscriber Identity	id-kp-clientAuth {1.3.6.1.5.5.7.3.2}; smartCardLogon {1.3.6.1.4.1.311.20.2.2}; id-pkinit-KPClientAuth {1 3 6 1 5 2 3 4} (Last two only if using a hardware Assurance Level)	None	All Others

Human Subscriber and Role Signature	id-kp-emailProtection
	{1.3.6.1.5.5.7.3.4};
	MSFT Document Signing
	{1.3.6.1.4.1.311.10.3.12};
	Adobe Certified Document Signing
	{1.2.840.113583.1.1.5}
		None	All Others

Human Subscriber and Role Encryption	Any EKU that is consistent with Key Usage, e.g., Encrypting File System {1.3.6.1.4.1.311.10.3.4}	Any EKU that is not consistent with Key Usage	All Others
Code Signing	id-kp-codesigning {1 3 6 1 5 5 7 3 3}	Life-time Signing {1.3.6.1.4.1.311.10.3.13}	All Others

Device Authentication, Web Server	id-kp-serverAuth
	{1 3 6 1 5 5 7 3 1}
	id-kp-clientAuth {1.3.6.1.5.5.7.3.2}
		None	All Others

Device Authentication Certificate used for Workstation	id-kp-clientAuth
	{1 3 6 1 5 5 7 3 2};
	iKEIntermediate
	{1 3 6 1 5 5 8 2 2};
	id-kp-ipsecIKE
	{1 3 6 1 5 5 7 3 17}
		None	All Others

Certificate Type	Required EKU	Optional EKU	Prohibited EKU
Device Signature used for Message Signing (Web Service, Type X, etc.), other than air-ground communications	id-messageSigning {1 3 6 1 4 1 11243 20 1 1}	None	All Others
Device Encryption used for Message Encryption (Web Service, Type X, etc.), other than air-ground communications	id-messageEncryption {1 3 6 1 4 1 11243 20 1 2}	None	All Others
Device Encryption used for Database Encryption	id-databaseEncryption {1 3 6 1 4 1 11243 20 1 3}	None	All Others

Certificate Type	Required EKU	Optional EKU	Prohibited EKU
Device Encryption used for Archive Encryption	id-archiveEncryption {1 3 6 1 4 1 11243 20 1 4}	None	All Others
Device Signature used for Archive Integrity Protection	id-archiveSigning {1 3 6 1 4 1 11243 20 1 5}	None	All Others
Device Signature used for Assertion Signing (e.g., SAML Assertions by Identity Providers and Attribute Authorities)	id-assertionSigning {1 3 6 1 4 1 11243 20 1 6}	None	All Others
Device Signature used for signing air-ground communication messages	id-airGroundCommsSigning {1 3 6 1 4 1 11243 20 1 7}	None	All Others
Device Encryption used for providing confidentiality to air- ground communication messages	id- {1 3 6 1 4 1 11243 20 1 8}	None	All Others

Certificate Type	Required EKU	Optional EKU	Prohibited EKU
Mediated Signature Certificate	None	Microsoft Document Signing {1 3 6 1 4 1 311 10 3 12}; Adobe Certified Document Signing {1 2 840 113583 1 1 5} id-fls-codesigning {1 3 6 1 4 1 11243 20 1 11} id-messageSigning {1 3 6 1 4 1 11243 20 1 1}	All Others
Device Signature	None	None	All
Device Encryption	None	None	All
High-cardAuth	id-PIV-cardAuth {2.16.840.1.101.3.6.8}	id-pivav-cardAuth {1 3 6 1 4 1 11243 20 1 9}	All Others
High-ContentSigning	id-fpki-High-content-signing {2.16.840.1.101.3.8.7}	id-pivav-contentSigner {1 3 6 1 4 1 11243 20 1 10}	All Others

Certificate Type	Required EKU	Optional EKU	Prohibited EKU

Domain Controller	id-kp-serverAuth
	{1 3 6 1 5 5 7 3 1};
	id-kp-clientAuth {1.3.6.1.5.5.7.3.2};
	id-pkinit-KPKdc
	{1 3 6 1 5 2 3 5};
	smartCardLogon {1.3.6.1.4.1.311.20.2.2 }
		None	All Others

Time Stamp Authority	id-kp-timestamping {1 3 6 1 5 5 7 3 8}	None	All Others
SCVP Server	id-kp-scvp-responder {1.3.6.1.5.5.7.3.15}	None	All Others
Web Client	id-kp-clientAuth {1.3.6.1.5.5.7.3.2}	None	All Others

Workstation	id-kp-clientAuth {1.3.6.1.5.5.7.3.2};
	iKEIntermediate {1.3.6.1.5.5.8.2.2};
	id-kp-ipsecIKE
	{1 3 6 1 5 5 7 3 17}
		None	All Others

Certificate Type	Required EKU	Optional EKU	Prohibited EKU

VPN Server	Id-kp-serverAuth
	{1.3.6.1.5.5.7.3.1}
	Id-kp-clientAuth
	{1.3.6.1.5.5.7417.3.2}
	iKEIntermediate
	{1.3.6.1.5.5.8.2.2}
	Id-kp-ipsecIKE
	{1.3.6.1.5.5.7.3.17}
		None	All Others

VPN Client	Id-kp-clientAuth
	{1.3.6.1.5.5.7.3.2}
	iKEIntermediate
	{1.3.6.1.5.5.8.2.2}
	Id-kp-ipsecIKE
	{1.3.6.1.5.5.7.3.17}
		None	All Others

ATN/IPS Ground Device Identity – ANSP	Id-kp-serverAuth {1.3.6.1.5.5.7.3.1}
	Id-kp-GroundIDANSP {TBD}
		None	All Others

ATN/IPS Ground Device Identity – AOC	Id-kp-serverAuth {1.3.6.1.5.5.7.3.1}
	Id-kp-GroundIDAOC {TBD}
		None	All Others

Certificate Type	Required EKU	Optional EKU	Prohibited EKU

ATN/IPS Ground Device Identity – IPS Gateway	Id-kp-serverAuth {1.3.6.1.5.5.7.3.1}
	Id-kp-GroundIDIPSGW {TBD}
		None	All Others

ATN/IPS Ground Device Identity – Content Provider	Id-kp-serverAuth {1.3.6.1.5.5.7.3.1}
	Id-kp-ContentProvider
	{TBD}
		None	All Others

ATN/IPS Aircraft Identity	Id-kp-clientAuth {1.3.6.1.5.5.7.3.2}
	Id-kp-aircraftID {TBD}
		None	All Others

3191

10.28 ENTITY TO PCA CROSS CERTIFICATE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	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 Entity)
Subject Key Identifier	c=no; Octet String (which is calculated as the SHA-1 hash of the BIT STRING subjectPublicKey, excluding the tag, length, and number of unused bits)
Key Usage	c=yes; keyCertSign, cRLSign,
Certificate Policies	c=no; {applicable policies}
Policy Mapping	c=no; {applicable policy mappings}
Basic Constraints	c=yes; cA=True; path length constraint absent
Name Constraints	c=yes; Optional, permitted subtrees for DN, RFC 5322, and DNS name forms
Policy Constraint	C=no; *inhibitPolicyMappings*, skip certs = 1

Field	Value
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to the ENTITY,; may contain id-ad-ocsp access method entry with HTTP URL for the ENTITY OCSP Responder
CRL Distribution Points	c = no;
Inhibit anyPolicy	c=no; skipCerts = 0

3195 ## 10.29 PCA TO ENTITY CROSS CERTIFICATE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	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 PCA)
Subject Key Identifier	c=no; Octet String (which is calculated as the SHA-1 hash of the BIT STRING subjectPublicKey, excluding the tag, length, and number of unused bits)
Key Usage	c=yes; keyCertSign, cRLSign,
Certificate Policies	c=no; {applicable policies}
Policy Mapping	c=no; {applicable policy mappings}
Basic Constraints	c=yes; cA=True; path length constraint absent
Name Constraints	c=yes; optional, excluded subtrees for DN, RFC 5322, and DNS name forms
Policy Constraint	C=no; *inhibitPolicyMappings*, skip certs = 1

Field	Value
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to PCA,; may contain id-ad-ocsp access method entry with HTTP URL for the PCA OCSP Responder
CRL Distribution Points	c = no;
Inhibit anyPolicy	c=no; skipCerts = 0

3198 10.30 ENTITY TO ANOTHER BRIDGE CROSS CERTIFICATE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	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 ICAB)
Subject Key Identifier	c=no; Octet String (which is calculated as the SHA-1 hash of the BIT STRING subjectPublicKey, excluding the tag, length, and number of unused bits)
Key Usage	c=yes; keyCertSign, cRLSign,
Certificate Policies	c=no; {applicable policies}
Policy Mapping	c=no; {applicable policy mappings}
Basic Constraints	c=yes; cA=True; path length constraint absent
Name Constraints	c=yes; optional, excluded subtrees for DN, RFC 5322, and DNS name forms
Policy Constraints	c=no; inhibitPolicyMapping skipCerts = 1

Field	Value
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to ENTITY,; may contain id-ad-ocsp access method entry with HTTP URL for the ENTITY OCSP Responder
CRL Distribution Points	c = no;
Inhibit anyPolicy	c=no; skipCerts = 0

3201 ## 10.31 ANOTHER BRIDGE TO ENTITY CROSS CERTIFICATE

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	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 Bridge)
Subject Key Identifier	c=no; Octet String (which is calculated as the SHA-1 hash of the BIT STRING subjectPublicKey, excluding the tag, length, and number of unused bits)
Key Usage	c=yes; keyCertSign, cRLSign
Certificate Policies	c=no; {applicable policies}
Policy Mapping	c=no; {applicable policy mappings}
Basic Constraints	c=yes; cA=True; path length constraint absent
Name Constraints	c=yes; optional, excluded subtrees for DN, RFC 5322, and DNS name forms
Policy Constraint	C=no; *inhibitPolicyMappings*, skip certs = 1

Field	Value
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Bridge,; may contain id-ad-ocsp access method entry with HTTP URL for the Bridge OCSP Responder
CRL Distribution Points	c = no;
Inhibit anyPolicy	c=no; skipCerts = 0

10.32 PKCS 10 REQUEST FORMAT

Field	Value
Version	V1 (0)
Subject Distinguished Name	Unique X.500 subject DN conforming to Section 7.1.4 of this CP
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Subject’s Signature	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Subject Key Identifier	c=no; Octet String
Key Usage	c=yes; (Optional) keyCertSign, cRLSign, digitalSignature, nonRepudiation
Basic Constraints	c=yes; optional; cA=True, path length constraint absent or 0 as appropriate
Name Constraints	c=yes; optional; permitted or excluded subtrees as appropriate for DN, RFC 5322, and DNS name forms

3207

10.33 DISTRIBUTION POINT CRL PROFILE

Field	Value
Version	V2 (1)
Issuer Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
thisUpdate	Expressed in UTC Time for dates until end of 2049 and Generalized Time thereafter
nextUpdate	Expressed in UTC Time for dates until end of 2049 and Generalized Time thereafter
Revoked Certificates list	0 or more 2-tuple of Certificate serial number and revocation date Expressed in UTC Time for dates until end of 2049 and Generalized Time thereafter
Issuer's Signature	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
CRL Extension	**Value**
CRL Number	c=no; monotonically increasing integer
Authority Key Identifier	c=no; Octet String (same as in Authority Key Identifier field in Certificates issued by the CA)
Issuing Distribution Point	c=yes; optional. Distribution point field must contain a full name (not relative name). The following fields shall all be absent: onlySomeReasons, indirectCRL, onlyContainsAttributeCerts
CRL Entry Extension	**Value**
Reason Code	c=no; optional unless circumstances were for reasons of key compromise or CA compromise
Hold Instruction	c=no; optional. id-holdinstruction-reject may be present only if reason code is CertificateHold

3208

10.34 SCVP SERVER PROFILE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11} or ecdsa-with-SHA384 {1.2.840.10045.4.3.2}
Issuer Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049 and Generalized Time thereafter
Subject Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1} or ecdsa-with-SHA384 {1.2.840.10045.4.3.2}
Issuer's Signature	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11} or ecdsa-with-SHA384 {1.2.840.10045.4.3.2}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as in Subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (which is calculated as the SHA-1 hash of the BIT STRING subjectPublicKey, excluding the tag, length, and number of unused bits)
Key Usage	c=yes; contentCommitment, digitalSignature
Extended Key Usage	C=yes; As per section 10.23
Certificate Policies	c=no; {applicable policies}
Subject Alternate Name	C=no; HTTP URL for the SCVP Responder

11. REFERENCES AND BIBLIOGRAPHY

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

ABADSG	Digital Signature Guidelines, 1996-08-01. http://www.abanet.org/scitech/ec/isc/dsgfree.html
ARINC 811	AEEC, Commercial Aircraft Information Security Concepts of Operation and Process Framework, December 20, 2005. http://www.aviation-ia.com/cf/store/catalog.cfm?prod_group_id=1&category_group_id=63
ARINC 823	AEEC, DataLink Security, Part 1 - ACARS Message Security, December 2007 http://www.aviation-ia.com/cf/store/catalog.cfm?prod_group_id=1&category_group_id=63
ARINC 842	Guidance for Usage of Digital Certificates http://www.aviation-ia.com/cf/store/catalog.cfm?prod_group_id=1&category_group_id=63
ATA iSpec2200 Air	Air Transport Association, Information Standards for Aviation Maintenance. http://www.ataebiz.org
AUDIT	FPKI Compliance Audit Requirements http://www.idmanagement.gov/documents/fpki-compliance-audit-requirements
CABF Base	CA Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.1, 14 Sep 2012. https://www.cabforum.org/Baseline_Requirements_V1_1.pdf
CABF EV	Guidelines for the Issuance and Management of Extended Validation Certificates, version 1.4, 29 May 2012. https://www.cabforum.org/Guidelines_v1_4.pdf
CCP-PROF	X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program. http://www.idmanagement.gov/fpkipa/documents/CertCRLprofileForCP.pdf
CIMC	Certificate Issuing and Management Components Family of Protection Profiles, version 1.0, October 31, 2001.
DIRECTIVE (EU) 2016/1148	Network and Information Systems Directive for Critical Infrastructure http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN
E-Auth	E-Authentication Guidance for Federal Agencies, M-04-04, December 16, 2003. http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf
ETSI EN 319 401	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers http://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.01.01_60/en_319401v020101p.pdf
ETSI TR 102 272	ASN.1 format for signature policies v1.1.1 http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=19571
ETSI TS 101 903	XML Advanced Electronic Signatures (XAdES) v1.4.2 http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=35243
ETSI TS 102 918	Associated Signature Containers (ASiC) version1.3.1 http://www.etsi.org/deliver/etsi_ts/102900_102999/102918/01.03.01_60/ts_102918v010301p.pdf
ETSI TS 319 132-1	Electronic Signatures and Infrastructures (ESI);Policy and security requirements for Trust Service Providers issuing Certificates version 1.1.1

	http://www.etsi.org/deliver/etsi_en/319100_319199/31913201/01.01.01_60/en_31913201v010101p.pdf
FIPS 140	Security Requirements for Cryptographic Modules, FIPS 140-2, May 25, 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
FIPS 140-2	Security Requirements for Cryptographic Modules May 25, 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
FIPS 186-5	Digital Signature Standard (DSS), FIPS 186-5, February 3,2023. https://csrc.nist.gov/publications/detail/fips/186/5/final
FIPS-197	National Institute of Standards and Technology, Advanced Encryption Standard, November 26, 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
FIPS 201	Personal Identity Verification (PIV) of Federal Employees and Contractors http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf and http://csrc.nist.gov/publications/drafts/fips201-2/Draft_NIST-FIPS-201-2.pdf
FOIACT	5 U.S.C. 552, Freedom of Information Act. http://www4.law.cornell.edu/uscode/5/552.html
FPKI-E	Federal PKI Version 1 Technical Specifications: Part E-X.509 Certificate and CRL Extensions Profile, 7 July 1997
FPKI-Prof	Federal PKI X.509 Certificate and CRL Extensions Profile
GDPR	General Data Protection Regulation http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=FR
IETF RFC 3647	Certificate Policy and Certification Practices Framework, Chokhani and Ford, Sabett, Merrill, and Wu, November 2003, https://tools.ietf.org/html/rfc3647
IETF RFC 4122	A Universally Unique IDentifier (UUID) URN Namespace, Paul J. Leach, Michael Mealling, and Rich Salz, July 2005. http://www.ietf.org/rfc/rfc4122.txt
IETF RFC 4210	Internet x.509 Public Key Infrastructure Certificate Management Protocol (CMP), C. Adams et. al. October 2005, http://www.ietf.org/rfc/rfc4210.txt
IETF RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, D. Cooper et. al, May 2008, http://www.ietf.org/rfc/rfc5280.txt
IETF RFC 5322	Internet Message Format, Peter W. Resnick, October 2008. https://tools.ietf.org/html/rfc5322
IETF RFC 6960	x.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, S. Santesson et. al., June 2013, https://tools.ietf.org/html/rfc6960
IETF RFC 7030	Enrollment over Secure Transport, M. Pritikin et. al., October 2013, https://www.ietf.org/mail-archive/web/ietf-announce/current/msg12045.html
ISO15408	Evaluation criteria for IT security, 2005, http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html
ISO9594-8	Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, 1997.
ITMRA	40 U.S.C. 1452, Information Technology Management Reform Act of 1996. http://www4.law.cornell.edu/uscode/40/1452.html
NAG69C	Information System Security Policy and Certification Practice Statement for Certification Authorities, rev C, November 1999.

NIST SP 800-37	Guide for the Security Certification and Accreditation of Federal Information Systems, NIST Special Publication 800-37, May 2004. http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf
NIST SP 800-53	NIST Special Publication 800-53: Recommendation for Security Controls for Federal Information Systems and Organizations http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3- final_updated-errata_05-01-2010.pdf
NIST SP 800-57	Barker et al., Recommendation for Key Management https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-4/final https://csrc.nist.gov/publications/detail/sp/800-57-part-2/final https://csrc.nist.gov/publications/detail/sp/800-57-part-3/rev-1/final
NIST SP 800-61	NIST Computer Security Incident Handling Guide, Rev 2. National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-61rev2/ SP800-61rev2.pdf
NIST SP 800-63-3	Digital Identity Guidelines https://csrc.nist.gov/publications/detail/sp/800-63/3/final
NIST SP-800-63A	Enrollment and Identity Proofing http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf
NIST SP-800-63B	Authentication and Lifecycle Management http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf
NIST SP-800-63C	Federation and Assertions http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf
NIST SP 800-73	Interfaces for Personal Identity Verification (4 Parts) http://csrc.nist.gov/publications/PubsSPs.html
NIST SP 800-73-3	Interfaces for Personal Identity Verification – Part 1: End-Point PIV Card Application Namespace, Data Model and Representation, NIST Special Publication 800-73-3, February 2010. http://csrc.nist.gov/publications/nistpubs/800-73-3/sp800-73-3_PART1_piv-card- applic-namespace-date-model-rep.pdf
NIST SP 800-76	Biometric Data Specification for Personal Identity Verification http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf
NIST SP 800-78	Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV) http://csrc.nist.gov/publications/nistpubs/800-78-2/sp800-78-2.pdf
NIST SP 800-88	NIST Special Publication 800-88: Guidelines for Media Sanitization http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf
NIST SP 800-122	Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) https://csrc.nist.gov/publications/detail/sp/800-122/final
NIST SP 800-147	NIST Special Publication 800-147, BIOS Protection Guidelines. April 2011. http://csrc.nist.gov/publications/nistpubs/800-147/NIST-SP800-147-April2011.pdf
NIST SP 800-147B	NIST Special Publication 800-147b, BIOS Protection Guidelines for Servers (Draft). July 2012. http://csrc.nist.gov/publications/drafts/800-147b/draft-sp800- 147b_july2012.pdf
NSD42	National Policy for the Security of National Security Telecom and Information Systems, 5 Jul 1990. http://snyside.sunnyside.com/cpsr/privacy/computer_security/nsd_42.txt (redacted version)
NS4005	NSTISSI 4005, Safeguarding COMSEC Facilities and Material, August 1997.

NS4009	NSTISSI 4009, National Information Systems Security Glossary, January 1999.
OECD	Guidelines on the Protection of Privacy and Transborder Flows of Personal Data http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsof personald ata.htm
OMB M-04-04	E-Authentication Guidance for Federal Agencies http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf
OMB M-07-16	Safeguarding Against and Responding to the Breach of Personally Identifiable Information http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf
PACS	Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems, Version 2.2, The Government Smart Card Interagency Advisory Board's Physical Security Interagency Interoperability Working Group, July 30, 2004. http://www.idmanagement.gov/smartcard/information/TIG_SCEPACS_v2.2.pdf
HIGH Profile	X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (HIGH) Cards, Date: April 23, 2010, http://www.idmanagement.gov/documents/High-x509-Certificate-and-Certificate-revocation-list-crl-extensions-profile
PKCS#1	Jakob Jonsson and Burt Kaliski, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, RFC 3447, February 2003. http://www.ietf.org/rfc/rfc3447.txt
PKCS#12	Personal Information Exchange Syntax Standard, April 1997. ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf
SCEP	Simple Certificate Enrollment Protocol http://www.ietf.org/internet-drafts/draft-nourse-scep-16.txt
SOAP	Simple Object Access Protocol v1.2 http://www.w3.org/TR/soap/
SSP REP	Shared Service Provider Repository Service Requirements. Federal PKI Policy Authority Shared Service Provider Working Group, December 13, 2011. http://www.idmanagement.gov/fpkipa/documents/SSPrepositoryRqmts.doc
TSCP	Transglobal Secure Collaboration Program (TSCP) Identity Federation Common Operating Rule v.1.4 http://www.tscp.org/wp-content/uploads/2013/11/tscp_idfed_cor_v.1.4.pdf
XML DigSig	XML Signature Syntax and Processing (Second Edition) http://www.w3.org/TR/xmldsig-core/

12. ACRONYMS AND ABBREVIATIONS

AES	Advanced Encryption Standard
AIA	Authority Information Access
AMS	ACARS Message Security
ANSI	American National Standards Institute
AOR	Authorized Organizational Representative
APL	Approved Product List
ARL	Authority Revocation List
ASN.1	Abstract Syntax Notation One Encoder / Decoder
ATA	Air Transport Association of America
C	Country
CA	Certification Authority
CARL	Certificate Authority Revocation List
CFR	Code of Federal Regulations
CHUID	Cardholder Unique Identifier
CIMC	Certificate Issuing and Management Components
CMC	Certificate Management over Cryptographic Message Syntax
CN	Common Name
COMSEC	Communications Security
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CSA	Certificate Status Authority

DC	Domain Component
DN	Distinguished Name
DNS	Domain Name Service
DP	Distribution Point
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
DUNS	Dun and Bradstreet
ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
FAA-WG	FAA Working Group
FIPS	(US) Federal Information Processing Standard
FIPS PUB	(US) Federal Information Processing Standard Publication
FPKI	Federal Public Key Infrastructure
FPKI-E	Federal PKI Version 1 Technical Specifications: Part E – X.509 Certificate and CRL Extensions Profile
FPKIPA	Federal PKI Policy Authority
GSA	General Services Administration
GUID	Globally Unique Identifier
HR	Human Resources
HSM	Hardware Security Module
HTTP	HyperText Transfer Protocol
ICAO	International Civilian Aviation Organization
ID	Identifier
IETF	Internet Engineering Task Force

IS	Information System
ISO	International Organization for Standardization
ITAR	International Traffic in Arms Regulation
KES	Key Escrow System
KRP	Key Recovery Policy
KRPS	Key Recovery Practices Statement
LOA	Level of Assurance
NATO	North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTP	Network Time Protocol
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
O	Organization
OA	Operational Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OMB	Office of Management and Budget
OTP	Onetime Password
OU	Organizational Unit
PCA	Principal CA
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure

PKIX	Public Key Infrastructure X.509
PMA	Policy Management Authority or PKI Management Authority
RA	Registration Authority
RCA	Root Certification Authority
RFC	Request For Comments
RP	Relying Party
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SCA	Subordinate CA
SCEP	Simple Certificate Enrolment Protocol
SCVP	Server-based Certificate Validation Protocol
SHA	Secure Hash Algorithm
SIA	Subject Information Access
STP	Signature Trust Platform
SCAs or Sub CAs	Subordinate Certificate Authorities
TA	Trusted Agent
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security
TSA	Time-stamp Authority
UPN	User Principal Name
UPS	Uninterrupted Power Supply
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
U.S.C.	United States Code
UTC	Coordinated Universal Time

UUID	Universally Unique Identifier (defined by RFC 4122)
VM	Virtual Machine
VME	Virtual Machine Environment
VPN	Virtual Private Network

13. GLOSSARY

Access	Ability to make use of any information system (IS) resource. [NS4009]
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009]
Activation Data	Private data, other than keys, that are required to access Cryptographic Modules (i.e., unlock Private Keys for signing or decryption events). *Note. Activation data is often a personal identification number (PIN) made up of numeric or alphanumeric characters.*
Administration Workstation	A workstation located outside the physical security perimeter of the CA and CSA used to administer CA and CSA equipment and/or associated Hardware Security Module (HSM).
Anonymous	Having an unknown name.
Affiliated Organization	Organizations that authorize affiliation with Subscribers.
Applicant	The Subscriber is sometimes also called an "Applicant" after applying to a certification authority for a Certificate, but before the Certificate issuance procedure is completed.
Archive	Long-term, physically separate storage.
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. 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.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009]
Authority Revocation List (ARL)	A list of revoked Certification Authority Certificates. Technically, an ARL is a CRL.
Authorized Organizational Representative (AOR)	A person (potentially among several) within an organization who is authorized to vouch for non-person identities. Any particular AOR is not permanently linked to any particular non-person identity; the CA must only ascertain that the AOR is legitimately associated with the organization, and that the AOR is identified as having authority for the identity in question.
Backup	Copy of files and programs made to facilitate recovery if necessary. [NS4009]
Binding	Process of associating two related elements of information. [NS4009]
Biometric	A physical or behavioral characteristic of a human being.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber's Public Key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]. As used in this CP, the term “Certificate” refers to Certificates that expressly reference the OID of this CP in the “Certificate Policies” field of an X.509 v.3 Certificate.
Certification Authority (CA)	Generally, an authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CARLs or CRLs. To that end, the Certification Authority is responsible for the following: 1.Control over the Subscriber registration, identification, and authentication process, 2.Signing of any Certificates and Cross Certificates it issues, 3.Verification that Subscriber possesses the Private Key that corresponds to the Public Key that shall be listed in the Subscriber’s Certificate,

	4. Publication of Certificates and Cross Certificates, 5. Revocation of Certificates and Cross Certificates, 6. Creation and digitally signing of Certificate Revocation Lists and/or Authority Revocation Lists, 7. Re-key of CA signing material, and 8. Ensuring that all aspects of the services, operations, and infrastructure related to the Certificates issued under its applicable CP are performed in accordance with the requirements, representations, and warranties of its CP. 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. A Certification Authority can perform the functions of a Registration Authority (RA) and can delegate or outsource this function to separate entities.
Certification Authority Revocation List (CARL)	See definition under Certificate Revocation List below.
Certificate Extension	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.
Certificate Policy (CP)	A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during Certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, Compromise recovery and administration of digital Certificates. Indirectly, a Certificate policy can also govern the transactions conducted using a communications system protected by a Certificate-based security system. By controlling critical Certificate Extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking and Renewing Certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).
Certificate Request	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. If the request is successful, the CA shall send back a Certificate that has been digitally signed with the CA's Private Key.
Certificate Revocation List (CRL) or Certification Authority Revocation List (CARL)	A list maintained by a Certification Authority of the Certificates, including Cross-Certificates which it has issued that are revoked prior to their stated expiration date. 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/CARL into a series of smaller CRLs/CARLs. 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/CARL.
Certificate Status Authority (CSA)	A trusted entity that provides on-line verification to a Relying Party of a subject Certificate's Revocation status and may also provide additional attribute information for the subject Certificate. Same as CMA (Certificate Management Authority).
Client (application)	A system entity, usually a computer process acting on behalf of a human user that makes use of a service provided by a Server.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]

Cross-Certificate	A Certificate is used to establish a trust relationship between two Certification Authorities. 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 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.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS1401]
Device	As used in Level of Assurance OIDs, a Non-Person Entity with a digital identity that acts in cyberspace but is not a human actor. This can include organizations, hardware devices, software applications, and information artifacts.
Digital Signature	The result of a transformation of a data by means of a cryptographic system using keys such that a Relying Party can determine: whether the transformation was created using the Private Key that corresponds to the Public Key in the signer's digital Certificate; and whether the message has been altered since the transformation was made.
Directory	A directory system that conforms to the ITU-T X.500 series of Recommendations.
Distinguished Name	A string created during the certification process and included in the Certificate that uniquely identifies the End-Entity within the CA domain.
Dual Use Certificate	A Certificate that is intended for use with both Digital Signature and data encryption services.
Encryption Certificate	A Certificate containing a Public Key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.
Encryption Key Pair	A public and Private Key Pair issued for the purposes of encrypting and decrypting data.

End-Entity (EE)	Relying Parties and Subscribers.
End Entity Certificate	A Certificate in which the subject is not a CA.
Entity	For the purposes of this document, “Entity” refers to an Organization, corporation, community of interest, or government agency with operational control of a CA.
Entity CA	A CA that acts on behalf of an Entity and is under the operational control of an Entity. The Entity may be an Organization, corporation, or community of interest. For the Federal Government, an Entity may be any department, subordinate element of a department, or independent organizational Entity that is statutorily or constitutionally recognized as being part of the Federal Government.
Employee	An Employee is any person employed in or by the Entity.
Federal Public Key Infrastructure Policy Authority (FPKIPA)	The FPKIPA is a United States federal government body responsible for setting, implementing, and administering policy decisions regarding inter Entity PKI interoperability that uses the FBCA.
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.
Firewall	Gateway that limits access between networks in accordance with local security policy. [NS4009]
Hardware Token	A hardware device that can hold Private Keys, digital Certificates, or other electronic information that can be used for authentication or authorization. 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).
Hypervisor	Computer software, firmware or hardware that creates and runs virtual machines. A Hypervisor uses native execution to share and manage hardware, allowing for multiple environments which are isolated from one another, yet exist on the same physical machine. Also known as an isolation kernel.

I-9 Form	An Employment Eligibility Verification form issued by the United States Department of Homeland Security whose purpose is to document verification of identity and employment authorization by employers.
Integrity	Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Issuing CA	In the context of a particular Certificate, the issuing Certification Authority is the Certification Authority that signed and issued the Certificate.
Integrated	Technologies exist that allow for the digital validation of identity evidence via electronic means (such as RFID to read the data directly from e-passports and chip readers for smartcards). The scanners and sensors employed to access these features should be integrated into the remote identity proofing stations in order to reduce the likelihood of being tampered with, removed, or replaced. To be integrated means the devices themselves are a component of the workstation (i.e., smartcard readers or fingerprint sensors built into a laptop) or the devices, and their connections, are secured in a protective case or locked box.
Internet Engineering Task Force (IETF)	The Internet Engineering Task Force is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.
Key Escrow	A deposit of the Private Key of a Subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the Subscriber, the terms of which require one or more agents to hold the Subscriber's Private Key for the benefit of the Subscriber, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"]
Key Generation	The process of creating a Private Key and Public Key Pair.
Key Management Key	Key exchange, key agreement, key transport

Key Pair	Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key
Key Recovery Policy (KRP)	A Key Recovery Policy is a specialized form of administrative policy that ensures the protection and recovery of key management Private Keys (i.e., decryption keys) held in escrow. A Key Recovery Policy addresses all aspects associated with the storage and recovery of key management Certificates.
Key Recovery Practice Statement (KRPS)	A statement of the practices that a key recovery system employs in protecting and recovering key management Private Keys, in accordance with the specific requirements specified in the relevant KRP.
Key Rollover Certificate	The Certificate that is created when a CA signs a new Public Key with an old Private Key, and vice versa.
Non-Person Entity	An entity with a digital identity that acts in cyberspace but is not a human actor. This can include Organizations, hardware devices, software applications, and information artifacts.
Non-Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009] Technical Non-Repudiation refers to the assurance a Relying Party has that if a Public Key is used to validate a Digital Signature, that signature had to have been made by the corresponding private signature key. Legal Non-Repudiation refers to how well possession or control of the private signature key can be established.
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI, they are used to uniquely identify each of the seven policies and cryptographic algorithms supported.
Online Certificate Status Protocol (OCSP)	Protocol useful in determining the current status of a digital Certificate without requiring CRLs.
Operational Authority (OA) Administrator	The Administrator is the individual within the Operational Authority who has principal responsibility for overseeing the proper operation of the CA infrastructure components, and who appoints individuals to other roles within the CA. The Administrator is selected by and reports to the PMA.

	The Administrator approves the issuance of Certificates to the other trusted roles operating the CAs.
Operational Authority (OA)	An agent of the Entity PKI CA. The Operational Authority is responsible to the PMA for: • Interpreting the Certificate Policies that were selected or defined by the PMA. • Developing a Certification Practice Statement (CPS), in accordance with the Internet X.509 Public Key Infrastructure (PKIX) Certificate Policy and Certification Practice Framework (RFC 3647), to document the CA's compliance with the Certificate Policies and other requirements. • Maintaining the CPS to ensure that it is updated as required. • Operating the Certification Authority in accordance with the CPS.
Organization	Department, agency, partnership, trust, joint venture or other association.
Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).
Person	A human being (natural person), corporation, limited liability company, or other judicial entity.
PIN	Personal Identification Number. See Activation Data for definition.
PKI Facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform Certificate issuance and Revocation.
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) or PKI Management Authority (PMA)	The individual or group that is responsible for the creation and maintenance of Certificate Policies consistent with x.509 Public Key Infrastructure (PKIX) Certificate Policy and Certification Practice Framework (RFC 3647), for developing methodology for approving applications for cross-certification, for accepting, processing and approving applications for cross-certification, and ensuring that all Entity PKI components (e.g., CAs, CSAs and RAs) are audited and

	continue to operate in compliance with the Entity PKI CP and any applicable TF CP. The PMA further evaluates non-domain policies for acceptance within the domain, and generally oversees and manages the PKI Certificate policies and provides policy direction to the CA and OA. The PMA is also responsible for approving agreements for cross-certification with external Certification Authorities. As specified in the applicable Charter, the PMA may be responsible for managing some dispute resolution amongst the PKI Entities.
Principal CA	CA within a PKI that has been designated to interoperate directly with another PKI (e.g., through the exchange of Cross-Certificates with a CA in another PKI domain). An Entity may designate multiple Principal CAs to interoperate with other CAs.
Privacy	Restricting access to Subscriber or Relying Party information in accordance with member States' privacy law and Entity privacy+ policy.
Private Key	The Private Key of a Key Pair is used to perform Public Key cryptography. This key must be kept secret. This can be: (1) The key of a Signature Key Pair used to create a Digital Signature. (2) The key of an Encryption Key Pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Pseudonym	A Subscriber name that has been chosen by the Subscriber that is not verified as meaningful by identity proofing. [NS4009]
Public Key	(1) The key of a Signature Key Pair used to validate a Digital Signature. (2) The key of an Encryption Key Pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital Certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, Server platforms, software and workstations used for the purpose of administering Certificates and Public-Private Key Pairs, including the ability to issue, maintain, and revoke Public Key Certificates.
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 RA is a Trusted Role that collects and verifies Applicant/Subscriber identity and information for inclusion in the Subscriber's Public Key Certificate. The RA is responsible for both identification and authentication of Certificate Subjects, but does not sign or issue Certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA). An RA interacts with the CA to enter and approve the Subscriber Certificate Request information. The Entity Operational Authority acts as the RA for the Entity Root and Sub CAs. Entity CAs shall designate their RAs, who must meet the requirements specified in the relevant CP.
Re-key (a Certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new Certificate on the new Public Key.
Relying Party	A person or entity who has received information that includes a Certificate and a Digital Signature verifiable with reference to a Public Key listed in the Certificate and is in a position to rely on them.
Renew (a Certificate)	The act or process of extending the validity of the data Binding asserted by a Public Key Certificate by issuing a new Certificate.
Repository	A database containing information and data relating to Certificates as specified in this CP; may also be referred to as a Directory.
Revocation	To prematurely end the Operational Period of a Certificate from a specified time forward.
Revoke a Certificate	To prematurely end the Operational Period of a Certificate effective at a specific date and time.
RFC 3647	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.
RFC 4122	Document published by the IETF which “[…] defines a Uniform Resource Name namespace for UUIDs (Universally Unique IDentifier), also known as GUIDs (Globally Unique IDentifier)”. (RFC 4122).
RFC 5280	Document published by the IETF which “[…] profiles the X.509 v3 Certificate and X.509 v2 Certificate Revocation List (CRL) for use in the Internet.” (RFC 5280)
Risk	An expectation of loss expressed as the probability that a particular Threat shall exploit a particular vulnerability with a particular harmful result.
Role Certificate	A Role Certificate is a Certificate, which identifies a specific role on behalf of which the human Subscriber is authorized to act.
Root CA	In a hierarchical PKI, the CA whose Public Key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Secure Enclave	The environment, which hosts the CA, KES and CSA equipment. The environment meets the physical and logical security requirements in this CP.
Server	A system entity that provides a service in response to requests from clients.
Server-based Certificate Validation Protocol (SCVP)	Protocol that allows a client to delegate Certificate path construction and Certificate path validation to a Server.
Signature Certificate	A Public Key Certificate that contains a Public Key intended for verifying Digital Signatures rather than encrypting data or performing any other cryptographic functions.
Signature Key Pair	A Public and Private Key Pair used for the purposes of digitally signing electronic documents and verifying Digital Signatures.
Signing CA	A CA whose primary function is to issue Certificates to End-Entities. A Signing CA is a Subordinate CA.
Signature Trust Platform	Service operated by the SSP (Signature Service Provider) -this is the European "Remote Signature Service" functionality as described in the ETSI regulations. A STP needs to be operated at the same level as a CA that issues the highest level of Certificates used by the STP.

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 Organization	An organization with which an Authorized Subscriber is affiliated (e.g., as an Employee, user of a service, business partner, customer etc.).
Subordinate CA	In a hierarchical PKI, a CA whose Certificate signature key is certified by another CA, and whose activities are constrained by that other CA.
Subscriber	A Subscriber is an entity that (1) is the Subject named or identified in a Certificate issued to that entity, (2) holds a Private Key that corresponds to the Public Key listed in the Certificate, and (3) does not itself issue Certificates to another party. This includes, but is not limited to, an individual or network device.
Subscriber Agreement	An agreement entered into by a Subscriber that provides the responsibilities and obligations of the Subscribers when using Certificates. Such agreement is a prerequisite in order to be able to use the Private Key associated to the Certificate.
Subject	The subject field of a Public Key Certificate identifies the entity associated with the Public Key stored in the subject Public Key field. Names and identities of a Subject may be carried in the subject field and/or the subjectAltName extension. Where subject field is non-empty, it MUST contain an X.500 Distinguished Name (DN). The DN MUST be unique for each subject entity certified by a single CA as defined by the issuer name field.
Supervised Remote Identity Proofing or Registration	A real-time identity proofing event where the RA or Trusted Agent is not in the same physical location as the Applicant or Subscriber, but controls a device used by the applicant or Subscriber in order to ensure the remote identity proofing process employs physical, technical and procedural measures to provide sufficient confidence that the remote session can be considered equivalent to a physical, in person identity proofing process.
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]
Time-Stamp Authority (TSA)	An authority that issues and validates trusted timestamps.

Token	A hardware security device containing an End-Entity’s Private Key(s) and Certificate. (see “Hardware Token”)
Trust List	Collection of Trusted Certificates used by Relying Parties to authenticate other Certificates.
Trusted Agent	Entity authorized to act as a representative of an Entity in confirming Subscriber identification during the Registration process. Trusted Agents do not have automated interfaces with Certification Authorities.
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
Two-Person or Multiparty Control	Continuous surveillance and -positive control of material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements. [NS4009]
Update (a Certificate)	The act or process by which data items bound in an existing Public Key Certificate, especially authorizations granted to the subject, are changed by issuing a new Certificate.
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.
Virtual Machine Environment	An emulation of a computer system (in this case, a CA) that provides the functionality of a physical machine and a platform-independent environment. It consists of a host (virtual machine) and isolation kernel (Hypervisor) and provides functionality needed to execute entire operating systems. For purposes of this policy, the definition of a virtual machine environment includes cloud-based solutions (e.g., platform-as-a-server) or container type solutions (e.g., Docker).
X.509	An ITU-T standard for a Public Key Infrastructure.
Zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS1401]