Federal Aviation Administration (FAA)

Non-Person Entity (NPE)

Certificate Practice Statement (CPS)

Redacted

Version 1.5

January 15, 2026

FAA Operational Authority (OA)

Name: Robert Segers

Title: NPE-IDMS System Owner

Signature: Signed by: Robert Segers

Signer Name: Robert Segers
Signing Reason: I approve this document
Signing Time: 1/21/2026 | 12:22:02 PM EST
651BEC09146149F09CA995389816FBDF

FOR OFFICIAL USE ONLY
Public availability to be determined under 5 USC 552

Revision History

Document Version	Document Date	Revision Details
.92	09/30/21	ICAO Doc 10169 Manual on Aviation Common Certificate Policy Baseline
.93	10/01/21	FAA Draft Baseline
.94	03/01/22	Updates through document to align with CP
.95	03/01/22	Updates through document to align with CP
.96	01/01/23	Updates through document to align with CP
.97	11/01/23	Updates through document to align with CP
.98	03/01/24	Updates through document to align with Auditors comments
1.0	06/12/2024	Version 1.0
1.1	07/12/2024	Updates to align with Key Ceremony Scripts
1.2	07/29/2024	Updates to align with WebTrust Controls
1.3	07/07/2025	Update to align with FAA NPE CP 1.2
1.4	08/19/2025	Update to align with FAA NPE CP 1.3 & 1.4
1.5	01/15/2025	Update Section 1.5.1 Contact Person

Table of Contents

1. INTRODUCTION

This Public Key Infrastructure (PKI) Certificate Policy (CP) and Certificate Practice Statement (CPS) defines multiple Assurance Levels for Certificates issued to Non-Person Entities (NPEs) hereafter "Device or Subscriber" 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. 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.

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

The CP defines several policies applicable to the use of digital Certificates for authentication, integrity (through digital signatures) and encryption to provide digital Certificates to Device End-Entities.

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

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

The CP and this CPS 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 the CPS outside the purview of the CA is completely at the Relying Party's Risk. An Entity will not assert the CA CPS 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.

The CPS 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 the CP and this CPS 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 the CPS means how certain a Relying Party (RP) can be of the identity Binding between the Public Key and the Device whose subject name is cited in the Certificate. In addition, it also reflects how certain the Relying Party can be that the Device 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 CPS. 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 Device, is confirmed via Out-of-Band communications.

Refer to:

- RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy
- CA-Browser-Forum-Network-Security-Guidelines-v1.7
- WebTrust® Principles and Criteria for Certification Authorities
- WebTrust® Secure Socket Layer (SSL) and Transport Layer Baseline with Network Security

1.1.1 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 the CP, which will be available to RPs. Each Certificate issued by the FAA will assert the appropriate level of assurance in the *CertificatePolicies* [1] extension.

1.1.2 Relationship between the CP and CPS

A CP states what assurance can be placed in a Certificate issued by the Certificate Authority (CA). This CPS states how the CA establishes that assurance. This CPS will always be aligned with the CP. It is mandatory for this CPS to maintain consistency with the CP, as this CPS is subordinate to the CP.

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

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

1.1.4 Scope

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

The Root CA will 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 and this CPS.

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

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

1.1.5 Interaction with PKIs External to FAA

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

---

[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 *italic* in this document.

1.2 DOCUMENT NAME AND IDENTIFICATION

This document is called the FAA Non-Person Entity Certificate Practice Statement (CPS).

There are five (5) levels of assurance Policy OIDs defined in Table 1 - FAA Certificate Policy Level of Assurance OIDs and OID Structure, in the NPE-IDMS CP 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 the CP and this CPS.

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 the FAA NPE CP documents the further sub-assignments.

Table 1 - FAA Certificate Policy 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		
CAB Forum - Domain Validated*	1	2.23.140.1.2.1
CAB Forum - Organization Validated	2	2.23.140.1.2.2
FAA CP	1	1.3.6.1.4.1.44109.0.1

*Reserved for future use.

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 CPS when referring to the Level of Assurance OIDs, the term "NPE" is defined as a Non-Person Entity (Device), 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 6.2.1

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.

Refer to:

- CPS Section 1.4.1 Appropriate Certificate Uses

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.

1.3.1 FAA PKI Authorities

The FAA Public Key Infrastructure (PKI) Management Authority (PMA) is defined in FAA Order J1370.121B.

1.3.1.1 PKI 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 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.

The FAA engages an independent auditors who specialize in PKI audits and can provide an objective evaluation of compliance with the offered PKI services. The auditors assess the operational practices, controls, and procedures implemented by the CA and verify their alignment with industry standards and best practices.

Refer to Section 8.1 Frequency of Audit or Assessments.

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 CP and this CPS and audit results
- Analyzing change requests for the CP and this CPS
- Recommending CP and this 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 OA that operate and maintain the CA on behalf of FAA, according to the CP and CPS.

The FAA engages an independent auditors who specialize in PKI audits and can provide an objective evaluation of compliance with the offered PKI services. The auditors assess the operational practices, controls, and procedures implemented by the CA and verify their alignment with the FAA CP and NPE-IDMS CPS with industry standards and best practices.

The 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.

1. Providing reasonable assurance that the CA Certificate Practice Statement (CPS) is updated annually and implements the latest version of the Certificate Policy (CP), WebTrust® for Certification Authorities WEBTRUST PRINCIPLES AND CRITERIA FOR CERTIFICATION AUTHORITIES, NETWORK SECURITY, and SSL BASELINE WITH NETWORK SECURITY requirements.
2. Assignment and periodic review of Trusted Roles.
3. Delegating the approval of issuance of NPE Certificates to Trusted Roles operating within the NPE-IDMS environment.
4. Establishing and maintaining NPE-IDMS system accounts and role segregation.
5. Configuring certificate profiles, templates, audit parameters, and ensuring that security requirements set by the CP and NPE-IDMS CPS, as well as Standard Operating Procedures (SOPs), are met.
6. Generating, managing, and backing up NPE-IDMS CA keys.
7. Ensuring the security of the NPE-IDMS environment, identifying.
8. Completing Training assignments, as required.
9. Requesting the PMA approval for the use of new facilities required for certificate authority information processing.
10. In the event of a disaster, notifying, and if needed, terminating affected entities and transferring relevant archived CA records from the affected entity to the NPE-IDMS Information Owner.

Refer to Frequency of Audit Assessments section 8.2.

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 the CP and this CPS are performed in accordance with the requirements, representations, and warranties of the FAA NPE 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 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 CPS may refer to CAs that are "subordinate" to the Principal CA. The use of the term "Subordinate CA" (SCA) will 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 will 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 will 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 Sub CA will be responsible for all aspects of the issuance and management of an End-Entity Certificate, as detailed in the CPS, 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 the FAA NPE CP and this CPS are performed in accordance with the requirements, representations, and warranties of the FAA NPE CP.

1.3.1.6 Root Certification Authority (RCA)

The FAA Root CA which will be called the RCA. The RCA will 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 the FAA NPE CP and this CPS are performed in accordance with the requirements, representations, and warranties of the 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 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 the FAA NPE CP and this CPS. Examples of CSA that fall within the scope of this CPS 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 use OCSP Servers that are locally trusted, as described in RFC 6960, (MC-OE JO-1370.123 example) will document FAA Relying party requirements in this 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 will 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 will 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 will follow security requirements detailed at other sections of FAA NPE CP and this CPS.

1.3.2 Registration Authorities

1.3.2.1 Registration Authority (RA)

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

In all cases, an RA will 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 will designate their RAs. The requirements for RAs in FAA PKI are set forth in Section 5.2.2.4.

1.3.3 Subscribers

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

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

1.3.3.1 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 will be indicated in a relative distinguished name in the subject field in the Certificate, and the Certificate will be revoked in accordance with Section 4.9.1 when affiliation is terminated.

1.3.3.2 Non-Person Entity (Device)

These are a broad class of physical and virtual entities which function on the network. NPE uses PKI authentication to validate their identity to other NPE or be authenticated to by other NPE 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.

1.3.3.3 Code Signer

A code signer is a Device 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 a Device. The Device Sponsor asserts that the Device will use the key and Certificate in accordance with the Certificate Policy asserted in the Certificate.

1.3.4 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 will 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.

The FAA NPE CP and this CPS 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.

1.3.5 Other Participants

1.3.5.1 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 CP and this CPS will identify the parties, define the services, and designate the mechanisms used to support these services.

1.3.5.2 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 will be verified in accordance with Section 3.2 and communicated to the RA in a secure manner.

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

1.3.5.3 Systems Administrator (SA)

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

1.3.5.4 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.

1.3.5.5 Compliance Auditor

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

1.3.5.6 Applicability

The sensitivity of the information processed or protected using Certificates issued by CAs will vary significantly. Relying Parties will 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 the FAA NPE Cp or this CPS.

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

1.3.5.7 Factors in Determining Usage

The Relying Party will first determine the level of assurance required for an application, and then select the Certificate appropriate for meeting the needs of that application. This will be determined by evaluating various Risk factors including the value of the information, the Threat environment, and the existing protection of the information environment. These determinations are made by the Relying Party and are not controlled by the 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.

1.3.5.8 Obtaining Certificates

Relying Party applications will 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

1.4.1 Appropriate Certificate Uses

To provide sufficient granularity, the CP which this CPS 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 the 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 (copied from FAA NPE CP)

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 3.2.3.4, Device 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 3.2.3.4, 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 Non-Person Entity Subscribers. See section 3.2.3.4, DEVICE 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 3.2.3.1, 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, Device 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 3.2.3.2, Individual Subjects

2376

2377 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 will be stored in hardware at this Assurance Level. Such Certificates will 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

1.4.2 Prohibited Certificate Uses

Refer to:

- CPS Section 9.17.1 Prohibited Certificate Use
- CPS Section 9.17.2 Corporate Controls

1.5 POLICY ADMINISTRATION

1.5.1 Organization administering the document

The PMA is responsible for all aspects of the CP and the OA is responsible for all aspects of the CPS.

1.5.2 Contact Person

Questions regarding the CPS will be directed to the Operational (OA), who can be reached at FAA Certificate Questions and Problem Report.

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 will be more detailed than the corresponding Certificate Policy. In all cases, the Certification Practices Statement will conform to the corresponding Certificate Policy.

The OA is responsible for asserting whether this CPS conforms to the 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.

Refer to:

- CPS Section 8 Compliance and Other Assessments

1.5.4 Certificate Practice Statement Approval Procedures

The OA will prepare and submit this CPS to the PMA for a determination that the CPS is consistent with the CP. If there are discrepancies, the identified discrepancies will be resolved, and this CPS will 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.

Refer to:

- CPS Section 9.10 Term and Termination
- CPS Section 9.12 Amendments

1.5.5 Waivers

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

1.6 DEFINITIONS AND ACRONYMS

Refer to:

- Appendix12 Acronyms and Abbreviations
- Appendix 13 Glossary

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

The OA operates the following repositories to support CA operations:

- **FAA PKI DOCUMENTS**

  Below are links to the FAA Certificate Policy and Certification Practice Statement (CPS) that have been approved by the FAA Policy Management Authority (PMA) and comply with CA Browser Forum TLS Baseline Requirements (BR) Version 2.0.2 and CA Browser Forum Network Security Controls Version 1.7 is located at:

  - http://idms-repository.faa.gov/

- **FAA CERTIFICATE AUTHORITIES**

  The Certificate Authorities (CRLs) authorized by the FAA PMA are located at: :

  - http://idms-repository.faa.gov/

- **FAA CERTIFICATE REVOCATION LISTS**

  The certificate revocation lists (CRLs) for FAA Public TLS Root and Issuing CAs is located at:

  - http://idms-repository.faa.gov/crl/

2.1.1 Repository Obligations

The repositories are accessible through HTTP.

The repositories include issued and valid end entity certificates, CA information, certificate revocation.

Access control and communication mechanisms to protect Repository information can be found in section 6.5.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

2.2.1 Publication of Certificates and Certificate Status

All Certificates are issued with valid URIs that are via HTTP port 80 accessible. There are no access controls imposed when these certificates are accessed by relying parties.

All NPE-IDMS repositories are safeguarded, and public-facing repositories serve as read-only proxies that mirror data stored securely behind advanced firewall protections. This architecture aligns with FAA security practices, guaranteeing both the security and auditability of our repositories.

The CA information repository contains the Authority Information Access (AIA) (CA certificates issued to the CA) and Subject Information Access (SIA) (CA certificates issued by the CA). The CRL and OCSP repositories contain certificate revocation information.

Encryption Public Key Certificates are not issued.

The OA ensures that CA Certificates and CRLs remain accessible 24/7/365, maintaining an availability rate of 99%.

The NPE-IDMS does not use a X.500 Directory Server System as a Repository.

Refer to:

- RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Framework

2.2.2 Publication of CA Information

A FAA approved redacted CPS containing no FAA confidential information is publicly accessible in the repository.

See section 2.1 Repositories.

2.2.3 Interoperability

There are no current plans or obligations to utilize X.500 or any directory for a Repository.

See section 2.1 and section 2.2.1

2.2.4 Privacy of Information

The CA and RAs will safeguard the privacy of Subscribers and Subscribers' Employers consistent with relevant laws and regulations. Subscribers and Subscribers' Employers authorize the CA or RAs to gather and utilize personal information, in accordance with section 9.4 and applicable law.

2.3 TIME OR FREQUENCY OF PUBLICATION

The CP and redacted CPS and any subsequent changes are made publicly accessible within thirty (30) days of PMA and OA approval respectively.

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

The CP and redacted CPS was published on June 14, 2024, before the first Certificate was issued.

2.4 ACCESS CONTROLS ON REPOSITORIES

The NPE-IDMS approach to securing repositories is comprehensive. All repositories are safeguarded, and public-facing repositories are essentially proxies, providing read-only access to copies of data stored securely behind firewalls. This method aligns with active security practices, ensuring both protection and auditability. The question of how access controls are implemented is addressed through these measures.

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

2.4.1 Certificate Policy

See section 2.2.2

2.4.2 Certificates and CRL

CAs will be the only entities authorized to create, modify, or otherwise maintain Certificates or CRLs. The authentication and protection mechanism used for these operations will be commensurate with the highest level of assurance issued by the CA. The Certificate Repository including certificates and CRLs will be protected against unauthorized modification.

The issuance of NPE-IDMS Trusted Role Z-PIV cards is governed by a strict authorization process that involves approval through a ticketing system, ensuring only personnel with necessary approvals

from operating authorities receive them. Further information for authentication and protection measures are found in:

3. IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

The CA generates and sign Certificates that contain a non-null subject Distinguished Name (DN). Certificates issued by the CA include alternative name forms.

Certificates issued by the CA, are in accordance with RFC 5280, and the following rules will be followed:

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

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

1) An Affiliated Organization name that is present in the Distinguished Name as an organization (o), organizational unit (ou), or domain component (dc) value.
2) Certificates that have no Affiliated Organization, the following rules apply:
   - "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.
3) For TLS Domain Validated Certificates, the organizational unit attribute will not be present.

Refer to:

- CPS Section 7.1.4.2 Name Forms for Organization

3.1.2 Need for Names to Be Meaningful

Issuing CAs will ensure that the Names in the Subject Distinguished Names (DNs) are comprehensible, adhere to name space uniqueness requirements, are not misleading, and can be easily interpreted by humans, which will be accomplished through the methods in the following subsections.

3.1.2.1 CA Certificates

The PMA will maintain a list of CAs and verify Name Uniqueness for new CAs.

3.1.2.2 Subscriber Certificates

The OA will configure the certificate and end entity profiles in the CA software to ensure DNs, including User Principal Names (UPNs) are unique names.

Distinguished Name compliance to the Name Forms in section 7.1.4 will be accomplished through the Name Form Template and End Entity and Certificate Profile configurations.

Subscribers will attest DNs, including User Principal Names (UPNs), accurately reflects the FAA Organizational structures.

Subscribers will attest that Roles provide clear and accurate depictions of functions executed by individuals (e.g., Purchasing Agent, System Administrator, etc.) within the Organizations.

For device certificates, the OA will ensure the meaningful names are either Fully Qualified Domain Names (FQDNs), IP addresses, URLs, model names/serial numbers, asset tags, or software applications using Name Form Templates and End Entity and Certificate Profile configurations.

For Organizations, the OA will ensure the meaningful names correspond to the legal names registered with the respective Registration or Incorporating Agencies.

Refer to:

- CPS Section 3.1.3: Anonymity or Pseudonymity of Subscribers
- CPS Section 7.1.5: Name Constraints

3.1.3 Anonymity or Pseudonymity of Subscribers

Certificates issued our NPE CAs do not contain anonymous or pseudonymous identities. All requests for device certificates are mandatorily linked to a verifiable FAA PIV personal identity, ensuring that each device's Distinguishable Names (DNs) are unique and identifiable. We prohibit the use of alterable information, such as IP addresses or URLs, for this purpose. We rely on non-changeable identifiers like serial numbers to serve as the foundation for each device’s DN, guaranteeing that each DN remains distinct and traceable.

3.1.4 Rules for Interpreting Various Name Forms

The CA has established the following rules for interpreting various Naming Forms:

The OA will maintain the CA and Subscriber Naming Forms with meaningful names based on name space constraints. The OA will approve these Naming Forms and report the name space for the Root, and Issuing CAs to the PMA.

The OA also will configure the certificate and end entity profiles in the CA software for End Entity Certificates based on the Certificate Profiles by reference as specified in Section 10 or a referenced certificate profile of the FAA NPE IDMS CP and this CPS.

Rules for interpreting name forms are defined in Certificate profiles referred to in this CPS Section 10.

3.1.5 Uniqueness of Names

Distinguished Name global uniqueness will be enforced by the FAA and the PMA. The OA will ensure that CA software is configured to not allow reuse of a distinguished name, ensuring uniqueness.

The CA will ensure that the Distinguished Name of a Subscriber remains unique even when multiple Certificates are issued to the same Subscriber.

The RAs will verify Device Sponsors, ensuring the uniqueness of names associated only once per End Entity Certificate using the Automated Subscriber Workflow Templates.

The Automated Subscriber Workflow contains a name uniqueness check. If a conflict is found, the Sponsor will be tasked to change the name, or the Workflow will append a number to the object's serial number.

3.1.6 Recognition, Authentication, and Role of Trademarks

The Subscribers and Device Sponsors acknowledge in the Certificate Request Workflows that they will not knowingly use names in the DNs of Certificate Application Request that infringe upon the intellectual property rights of others.

The CA reserves the right to make all decisions regarding Subscriber names in all assigned Certificates. The CA operating under the CP and this CPS is not 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 the CP and this CPS is entitled, without liability to any Subscriber, to reject or suspend any Certificate because of such dispute.

3.1.7 Name Claim Dispute Resolution

In case of any name collisions or disputes, the CA consults with the PMA and works with the sponsor to resolve the name collision.

The CAs will not knowingly use trademarks in names unless the Subject has the rights to use that name, in accordance with the section 9.5.3.

Refer to:

- CPS section 3.1.6 Recognition, Authentication, and Role of Trademarks.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

The Certificate Authority does not record the private keys in any form (e.g., plaintext or enciphered).

When the CA requests that the Device Sponsor prove possession of the Sponsor's private key and the device sponsor cannot or will not, the CA will revoke the certificate within 24 hours through the Certificate Revocation Form process.

3.2.2 Authentication of Organization Identity

At present, the CA does not actively implement the issuance of cross-certificates and will require implementation and PMA approval when needed.

3.2.3 Authentication of Individual Identity

3.2.3.1 NPE Subjects

This CPS describes procedures that will be implemented to ensure that all Certificate accountability is maintained.

The Sponsor Organization will ensure to request of transfer of sponsorship to a new Device Sponsor when the current Device Sponsor no longer has this role.

In the case of a change in Device Sponsor, the new Sponsor will be required to review the status of each NPE under their sponsorship to ensure it is still authorized to receive Certificates..

3.2.3.2 Individual Subjects

The CA validates the identity of Device Sponsors through the following methods:

The Trusted Agents and Registration Authorities rely on the FAA PIV antecedent process (see CPS section 3.2.3.5) to validate the identity of Device Sponsors for End Entity Certificates at both Low and Medium Assurance Levels ensuring the FAA Device Sponsor's PIV identity information and Public Key are properly bound.

This PIV antecedent process will require Device Sponsors to have a valid FAA PIV card and PIN and current Active Directory (AD) account and authenticate to the FAA at LOA 4, grant access to the Certificate Request Form and the date and time of when the verification occurred.

Refer to 3.2.3.5 Human Subject Identity Proofing via Antecedent Relationship

3.2.3.3 Individual Subject for Role Certificates

Not applicable.

3.2.3.4 Individual Subject for *TSP Mediated Signature* Certificates

Not applicable.

3.2.3.5 Human Subject Identity Proofing via Antecedent Relationship

The Certification Authority (CA) will use the FAA Security and Hazardous Material Safety (ASH) Personal Identity Verification (PIV) process to validate the identities of the Operational Authority (OA), Subscribers, and Device Sponsors:

OA Validation PIV Process:

- The PIV process adheres to NIST Special Publication 201 and includes verification of:
  - Full legal name (given and surname) from government-issued ID documents.
  - Birth date from government-issued ID documents, to uniquely identify the Human Sponsor.
  - Physical street address from government-issued ID documents.
  - Unique ID number assigned to the government-issued ID documents.
  - Affiliated Organizations entered by Human Sponsor.
  - Email address entered by Human Sponsor.
- The process also records:
  - Unique ID number assigned to the government-issued ID documents.
  - Date and time of the validation.

FAA Subscriber and Device Sponsor Validation:

- The Trusted Agents (TAs) and Registration Authorities (RAs) will rely on FAA PIV validation to verify the identity of FAA Subscribers and FAA Device Sponsors for End Entity Certificates at the Low and Medium Assurance Levels.
- After authenticating to the RA NPE workflow with FAA accounts, the FAA Device Sponsors are required to fill in, digitally certificate sign, and submit a Certificate Application Request for End Entity Certificates. These forms include a declaration of identity and an acceptance of the terms outlined in section 9.6.3.
- Both the TAs and RAs independently verify this information and digitally certificate sign the Certificate Application Request in the RA NPE workflow.

Operational Authority Documentation:

- The OA signs the Operational Trusted Roles Charter document, which includes a declaration of identity and an acceptance of the Privacy Policy (refer to section 9.6.3).

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

The CA will ensure that only verified information has been included in the Certificates through the following methods:

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 that are the same as those followed for the initial identity proofing Section 3.2.3.1 or Section 3.2.3.2 with the following modifications:

- The validity period of the Certificates issued using this process will not exceed the identity-reproofing requirements in Section 3.3.1.
- Only one National Government-Issued Photo ID or non-National Government issued Photo ID (e.g., Driver's License, Passport) is required.

3.2.4 Non-verified Subscriber Information

The OA will verify all information included in Certificate requests and Certificates using the NPE Workflow.

3.2.5 Validation of Authority

At present, the CA does not actively implement the issuance of cross-certificates and will require implementation and PMA approval when needed.

3.2.6 Criteria for Interoperation

At present, the CA does not actively implement the issuance of cross-certificates and will require implementation and PMA approval when needed.

The cross-certification criteria methodology includes specific verifications to ensure compliance with the CP. These verifications include:

- Completion of CP-to-CP mapping and finding the CPs to be equivalent.
- Successful passing of a Compliance Audit by the CA (as outlined in Section 8 of the CP).
- Verification of compliance of Certificate Profiles and Certificates with the applicable CP.
- Verification of compliance of Certificate Status (e.g., CRL, OCSP) with the applicable CP.
- Verification that CA Certificates and Certificate Status information are published and available for Relying Parties.

Interoperating CAs will be required to adhere to the following requirements:

- Complete policy mapping with the CA CP to the satisfaction of both parties.
- Operate a CA that has successfully undergone a Compliance Audit, as specified in Section 8 of the CP and the Subject CA's CP.
- Issue Certificates compliant with the profiles described in the CP, and this CPS and make Certificate status information available in compliance with the CP and CPS.
- Assert the Certificate Policy OIDs as outlined in Section 1.2.2.
- Publish CA Certificate and Certificate status information.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-key

The CA will validate Device Sponsors to routinely re-key CA, Cross, and End Entity Certificates through the following methods:

3.3.1.1 End Entity Certificates

Device Sponsors have two (2) options to renew End Entity Certificates.

- The first option is to generate public/private key pairs and CSRs for the Devices (*e.g.*, web servers, aircraft avionics, etc.).
- The second option is to request the CA software to produce public/private key pairs and CSRs.
- For Device Identity Certificates issued, the TAs and RAs will perform identity validation of Device Sponsors every year as specified in Section 3.2.3.1.

TAs and RAs will re-validate the identities of Device Sponsors every three (3) years or for Device Identity Certificates every three hundred ninety-seven (397) days.

3.3.2 Identification and Authentication for Re-key after Revocation

After a Certificate has been revoked, except for cases such as renewal, update, or replacement of a lost/stolen/damaged credential, the Device Sponsor must undergo the initial registration processes described in Section 3.2.3 and 3.2.3.2 to obtain a new Certificate. However, if the Device Sponsor can be authenticated with a non-revoked Certificate of equal or higher assurance issued by the same CA, the initial registration process may be bypassed.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Certificate revocation request will be made using a revocation workflow template. Access to the workflow template will use the PIV authentication.

The CA or RA will 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.

The revocation requested will be logged in the Approved Certificate Database with the Revocation envelope ID.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

This section specifies requirements for initial application for Certificate issuance.

4.1.1 Submission of Certificate Application

For Device certificates, Device Sponsors submit a Certificate Application Request to issue, renew, or modify Certificates.

4.1.1.1 Application for Organizational Certificates

Not applicable.

4.1.1.2 Application for Subscriber Certificates by an individual

Not applicable.

4.1.1.3 Application for Subscriber Certificates on behalf of a NPE

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

4.1.1.4 Application for *TSP Mediated Signature* Certificates by an Individual

Not applicable.

4.1.1.5 Application for CA Certificates

The CA Naming Forms will capture the required information and documentation as defined in this CPS Sections 3.2.2 and 3.2.3. The OA will prepare and submit the CA Naming Forms to the PMA.

4.1.2 Enrollment Process and Responsibilities

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

Applicants will be required to self-attest the information provided in the certificate application is accurate information.

4.1.2.1 Subscriber Certificates

The Applicant and the RA will 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.

4.1.2.2 CA Certificates

Entity CAs will only issue Certificates asserting the OIDs outlined in the CA CP upon receipt of an approved CA Naming Form from the OA, and only do so within the constraints imposed by the PMA.

4.2 CERTIFICATE APPLICATION PROCESSING

Information in Certificate applications will be verified as accurate before Certificates are issued as described in section 4.1.2 Enrollment Process and Responsibilities.

The RA will verify that the information in a Device Certificate Application is accurate.

The RA will verify that the information in a CA Certificate Application is accurate.

4.2.1 Performing Identification and Authentication Functions

The CA will verify the identity and authority of Subscribers and Device Sponsors via the following methods:

4.2.1.1 CA Certificates

For CA Certificates, the OA will verify the Organizations, confirm ownership of Domain Names, and validate the identity of Subscribers as defined in Section 3.2.3. Further, the OA validate the authority of Subscribers to request CA Certificates on behalf of Organizations as defined in Section 3.2.5.

Refer to:

- CPS Section 3.2.2 Authorization of Organization and Domain/Email Control
- CPS Section 3.2.3 Authorization of Individual Identity
- CPS Section 3.2.5 Validation of Authority
- RFC 8659 DNS Certification Authority Authorization (CAA) Resource Record

4.2.1.2 End Certificates

For End Entity Certificates, the TAs and RAs will rely on Device Sponsors authenticating to the RA software to submit Certificate Application Request. This authentication will require the Device Sponsors to obtain an FAA account which verifies the identity of Device Sponsors as defined in Section 3.2.3. The TAs and RAs will check information about Organizations and Domain Names in the Certificate Application Request as defined in Section 3.2.2. In addition, the TAs and RAs will confirm the authority of the Device Sponsors as defined in Section 3.2.5.

Refer to:

- CPS Section 3.2.2 Authentication of Organization and Domain/Email Control
- CPS Section 3.2.3 Authentication of Individual Identity

4.2.2 Approval or Rejection of Certificate Applications

The CA will approve or rejects the Certificate Applications through the following methods:

For CA Certificates, the OA will approve or reject the CA Naming Forms.

Refer to:

- CPS Section 3.2.3 Authentication of Organization and Domain/Email Control
- CPS Section 3.2.3 Authentication of Individual Identity

For End Entity Certificates, the TAs and RAs will approve or reject the Certificate Application Request in the RA software. The TAs and RAs will reject the Certificate Application Request for the following reasons:

- TAs or RAs cannot validate information and/or documentation about Organizations, Subscribers, or Domain Names
- Subscribers fail to provide requested information or documentation
- Subscribers do not send requested information or documentation within timeframe specified by the RAs
- TAs or RAs discover inaccuracy in the information or documentation
- TAs or RAs find Organizations or Subscribers on sanctions list in section 9.17.1
- TAs or RAs recognize trademarks belong to other Organizations
- No appropriate charge numbers for certificate payment

Refer to:

- CPS Section 3.2.2 Authentication of Organization and Domain/Email Control
- CPS Section 3.2.3 Authentication of Individual Identity

4.2.3 Time to Process Certificate Applications

Individual Identity will be confirmed no more than 90 days before initial Certificate issuance which will be enforced by the Certificate Application Request workflow.

4.3 CERTIFICATE ISSUANCE

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

The OA will ensure there is an auditable chain of custody when information is obtained through one or more data sources, through periodic internal audit of audit logs.

4.3.1 CA Actions during Certificate Issuance

For End Entity certificates, the CA will authenticate the source of Certificate Request before issuance as per section 3.2.3.2 Individual Subjects. Certificates will be checked by the CA software to ensure that all required fields and extensions are properly populated. After generation, verification, and acceptance the CA will publish the Certificate in the certificate Repository, see Section 2.1 REPOSITORIES. This will all be done within 1 hour.

For CA Certificates, the CA will authenticate the source of Certificate Request before issuance as per section 4.2.1.1 CA Certificates. Certificates will be manually checked to ensure are fields and extensions are properly populated. After generation, verification, and acceptance the CA will publish the Certificate in the CA Information AIA and SIA repositories, see section 2.1 REPOSITORIES. This entire process will occur within 24 hour.

4.3.2 Notification to Subscriber of Certificate Issuance

For CA Certificates, notification and delivery of certificates will be accomplished by Certificate Request Form.

4.4 CERTIFICATE ACCEPTANCE

The Device Sponsor signs the Certificate Request Form and acknowledges the issuance of the Certificate and the Device Sponsor's responsibilities as defined in Section 9.6.3.

4.4.1 Conduct Constituting Certificate Acceptance

A Subscriber will explicitly indicate acceptance of the Certificates within 45 days by acknowledging receipt of the certificate. If the CA does not receive explicit acknowledgement within 45 days, it will revoke the certificate.

For CA Certificates, during key ceremonies, the OA will receive CA Certificates as PKCS#7 files from the CA software. The OA will verify content of PKCS#7 files as defined in the key ceremony scripts and accepts the CA certificate in accordance with the CA Naming Form.

4.4.2 Publication of the Certificate by the CA

See section 4.3.1 CA Actions during Certificate Issuance. There is no need to publish *TSP Mediated Signature* Certificates.

4.4.3 Notification of Certificate Issuance by the CA to other entities

For publicly trusted CA Certificates, the OA will notify the CA/B Forum to enroll the CA Certificates in the Mozilla, Windows, Google, and Apple Root Programs.

The PMA will be notified through email for all cross-certified entities of all new artifacts (e.g., CA Certificates, CRL DP, AIA and/or SIA URLs, etc.) within 24 hours of issuance.

The PMA will be notified by email from the OA at least two weeks and a day prior to the issuance of any new CA Certificate or external CA Certificates.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

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

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

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties must 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 will, 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.

4.5.3 Device Sponsor Private Key and Certificate Usage

See section 4.5.1 Subscriber Private Key and Certificate Usage.

4.6 CERTIFICATE RENEWAL

4.6.1 Circumstance for 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, but must not be further re-keyed, Renewed or modified.

The CA certificate renewal procedures do not allow for replacing OCSP Responder Certificates, SCVP Responder Certificates, Cross-Certificates, and Device Certificates where the Certificate lifetime is purposely shorter than the Private Key lifetime.

4.6.2 Who may request Renewal

For Cross Certificates, the OA will request the PMA for approval to renew CA Certificates.

For End Entity Certificates, the Device Sponsors must submit requests to renew End Entity Certificates.

Device Sponsors can request renewal of their own device certificates through the automated Certificate Request Form.

4.6.3 Processing Certificate Renewal Requests

The CA will process Certificate Requests for renewals as defined in Section 3.3.1.

The Certificate keys do not change during the renewal process.

4.6.4 Notification of new Certificate issuance to Subscriber

The CA will notify Device Sponsors about issuance of Certificates as defined in Section 4.3.2.

4.6.5 Conduct constituting acceptance of a Renewal Certificate

The CA will require Device Sponsors to accept or reject Certificates as defined in Section 4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

The CA will publish the renewed Certificates in Repositories as defined in Section 4.4.2.

4.6.7 Notification of Certificate Issuance by the CA to other entities

The CA will notify other Entities as defined in Section 4.4.3.

4.7 CERTIFICATE RE-KEY

The NPE CA will only issue new certificates and will not be further re-keyed, Renewed, or modified.

4.7.1 Circumstance for Certificate Re-key

The OA re-key CA and Cross Certificates based on meeting all the following conditions:

- The associated Public Keys have not exceeded Not After field in the Certificates
- The associated Private Keys have not been compromised
- The Certificates have not been revoked

The CAs and RAs may initiate Re-key of a Subscriber's Certificates without a corresponding request from the Subscriber or Sponsor through the automated Certificate Request Form.

4.7.2 Who may request certification of a new Public Key

For Cross Certificates, the OA will submit a request to the PMA for approval to re-key CA Certificates.

For End Entity Certificates, the Device Sponsors will be required to submit requests to re-key End Entity Certificates.

4.7.3 Processing Certificate Re-keying requests

For the CA, the OA must verify that the validity period associated with the new Certificate does not extend beyond the term of the (See section 1.3.1.1).

The CA will process Certificate Requests for re-keys as defined in Section 3.3.1.

4.7.4 Notification of new Certificate issuance to Subscriber

The CA will notify Device Sponsors about issuance of Certificates as defined in Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a re-keyed Certificate

The CA will require Device Sponsors to accept or reject Certificates as defined in Section 4.4.1.

4.7.6 Publication of the Re-Keyed Certificate by the CA

The CA will publish the re-keyed Certificates in Repositories as defined in Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to other Entities

The CA will notify other Entities as defined in Section 4.4.3.

4.8 CERTIFICATE MODIFICATION

4.8.1 Certificate Modification is only supported for CA Certificates.

Not applicable.

4.8.2 Who may request Certificate Modification

Not applicable.

4.8.3 Processing Certificate Modification Requests

Not applicable.

4.8.4 Notification of new Certificate issuance to Subscriber

Not applicable.

4.8.5 Conduct constituting acceptance of modified Certificate

Not applicable.

4.8.6 Publication of the modified Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate issuance by the CA to other Entities

Not applicable.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 OA Circumstances for Revocation

For CAs, a Certificate will be revoked when the Binding between the Subject and the Subject's Public Key defined within a Certificate is no longer considered valid. When that occurs, the PMA will meet as soon as practicable to review an emergency revocation.

Whenever any of the above circumstances occur, the associated Certificate is revoked and placed on the CRL.

Revoked Certificates are included on all new publications of the Certificate status information until the Certificates expire.

Refer to:

- CA/B Forum Baseline Requirements 6.1.5 Key Sizes
- CA/B Forum Baseline Requirements 6.1.6 Public Key Parameters Generation and Quality Checking

4.9.2 Who Can Request Revocation

The CA will accept Revocation Requests from Device Sponsors for their Device Certificates, Role Sponsors, and Affiliated Organizations. The CA may also consider request for revocation from other parties (e.g., supervisors, Human Resources, operational personnel).

The CA reserves the right to revoke Certificates at their sole discretion. The CA will also revoke a CA Certificate at the direction of the PMA.

4.9.3 Procedure for Revocation Request

For End Entity certificates, the Device Sponsor must authenticate to using their PIV credential for authentication and validation to allow access to the Revocation Request Form. The Device Sponsor enters certificate information and a reason for revocation and submits the Revocation Form to the RA for approval. The RA will review and approves the Revocation request. The next step in the Revocation Request Form workflow is for the CA software to revoke the certificate.

Refer to:

- CPS Section 1.5.2 Contact Person

- CPS Section 4.9.1 Circumstances for Revocation

4.9.4 Revocation Request Grace Period

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

4.9.5 Time within which CA must Process the Revocation Request

The Time within which CA must Process the Revocation Request does not allow a Revocation grace period. Responsible parties will be required to request Revocation as soon as they identify the need for Revocation Time within which CA must Process the Revocation Request

All Revocation requests will be processed within 24 hours of receipt of request.

The Online CA will revoke Certificates before the next CRL is published, except when the request is validated within two (2) hours of CRL issuance. Revocation requests validated within two (2) hours of CRL issuance will be processed before the following CRL is published.

Revocation request processing time required in the CP is 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 request processing time may be further constrained by applicable law.

Refer to:

- CPS Section 4.9.1 Circumstance for Revocation

4.9.6 Revocation Checking Requirements for Relying Parties

The Relying Parties are responsible for confirming validity of Certificates relying parties to check for a refreshed CRL every 24 hours for the latest Cross-Certificate Revocations in accordance with IETF PKIX standards before relying on the information contained within Certificates. This confirmation should include the following checks:

- Verifying the status of End Entity and CA Certificates in the chain via CRL or OCSP
- Validating Authority Key Identifier (AKI) and Subject Key Identifier (SKI) fields
- Checking Key Usage and Extended Key Usage (EKU) fields
- Confirming Policy Constraints

4.9.7 CRL Issuance Frequency

The CA software will generate new CRLs of all unexpired, revoked Certificates. Also, the CA software will remove expired Certificates from CRL files.

For offline Issuing CAs (*i.e.*, Root CA), the OA will manually update and issue new CRLs at least once every 12 months in the CA software. When Subordinate CA Certificates have been revoked, the

OA manually update and re-issue CRLs within 24 hours in the CA software. The nextUpdate field is not more than 12 months beyond the thisUpdate field of the CRLs.

For the online Issuing CA, the CA software will automatically updates and issues a new CRL every 24 hours, unless Key Compromise occurs in which case the CRL is updated immediately, but no later than 18 hours.

4.9.8 Maximum Latency of CRLs

The CA software will publish new CRLs to the Repositories within four (4) hours after generation and no later than the time specified in the nextUpdate field of the previously issued applicable CRL,, ensuring the CRL is available to Relying Parties with 24 hours of validation of the revocation request.

The OA archives the previous CRL.

4.9.9 On-line Revocation/Status Checking Availability

The CA software will ensure OCSP Responses meet or exceed the CRL issuance and frequency requirements. The OCSP Response times will be no longer than ten (10) seconds.

The OCSP Response will conform to RFC 5019 and/or RFC 6960 and is signed by either:

1. Issuing CA that issued the Certificates whose revocation status is being checked; or
2. OCSP Responder whose Certificate is signed by the Issuing CA that issued the Certificate whose revocation status is being checked.

When signed by an OCSP Responder, the OCSP Responder Certificate will contain the id-pkix-ocsp-nocheck extension as defined by RFC 5019 and/or RFC 6960.

Refer to:

- CPS Section 4.9.5 Time in Which the CA Must Process Revocation Request
- CPS Section 4.9.7 CRL Issuance Frequency
- CPS Section 4.9.8 Maximum Latency of CRLs
- RFC 5019 The Lightweight Online Certificate Status Protocol (OCSP) Profile for High Volume Environments
- RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP

4.9.10 On-line Revocation Checking Requirements

The OCSP Responders support the HTTP GET method as described in RFC 5019 and RFC 6960.

The validity interval in OCSP Responses is the difference in time between the thisUpdate and nextUpdate fields. For the purposes of computing differences, 3,600 seconds is equal to one (1) hour, and 86,400 seconds is equal to one (1) day ignoring leap-seconds.

A list of OCSP Responders is published in the PKI Repository.

Refer to:

- RFC 5019 The Lightweight Online Certificate Status Protocol (OCSP) Profile for High Volume Environments

- RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP

4.9.11 Other Forms of Revocation Advertisements Available

No alternative method will be used to publicize revocation of Certificates.

4.9.12 Special Requirements Related to Key Compromise

The OA notifies through digital signed email the PMA and Device Sponsors within 18 hours if the CA signing key is compromised or suspected of compromise. See Section 4.9.7

4.9.13 Circumstances for Suspension

Not applicable. The CA will not suspend Certificates.

4.9.14 Who can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension / Un-Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

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 are optional.

4.10.1 Operational Characteristics

Both CRL and OCSP Responder will be ascertained by HTTP queries.

4.10.2 Service Availability

The CA operates the Repositories storing CRLs and OCSP Responses on a 24x7x365 basis with 99% availability. Also, The CA ensures the CRLs and OCSP Responses have a ten (10) second or less response time under normal operating conditions

Additionally, The CA will maintain a public Certificate Problem Report web page that is available on a 24x7x365 basis with 99% availability to request revocation of problematic Certificates. The CA monitors new Certificate problem reports on a 24x7x365 basis. Lastly, the CA will forward high priority Certificate problem reports to law enforcement and revoke high priority, problematic Certificates on a 24x7x365 basis.

4.10.3 Optional Features

No stipulation

4.11 END OF SUBSCRIPTION

Not applicable.

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policy and Practices

Not applicable. The CA will not perform any escrow or key recovery functions.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. FACILITY, MANAGEMENT AND OPERATIONS CONTROLS

5.1 PHYSICAL CONTROLS

5.1.1 Site Location and Construction

The OA will implement measures to ensure the physical security of the CA facilities. These measures are designed to:

- Limit physical access to OA facilities and equipment to authorized individuals, utilize multi-factor authentication controls and protected by restricted security perimeters.
- Shield OA facilities and equipment from environmental hazards.
- Avert loss, damage, or compromise of assets and business activities interruptions.
- Prevent compromise of information and information processing facilities.

5.1.2 Physical Access

5.1.2.1 Physical Access for CA Equipment

All CA personnel will be authorized for physical access to the CA equipment via a CA physical access authorization process requiring the OA approval.

5.1.2.2 Physical Access for RA Equipment

The RA equipment is protected using the same security controls as the CA equipment. See in Section 5.1.2.1.

5.1.2.3 Physical Access for CSA Equipment

The CSA equipment is housed in the 2 person access control rack described in Section 5.1.2.1 and as such follows the requirements specified in Section 5.1.2.1.

5.1.3 Power and Air Conditioning

The OA has contracted with Equinix and AWS to provide backup capability sufficient to automatically finish any pending tasks and record the state of CA, RA, and CSA systems before lack of power or air conditioning causes a shutdown.

5.1.4 Water Exposures

The OA has implemented industry's best practices to protect the CA systems from water exposure which includes raised floors for the cages and cabinets storing CA systems, use of tables to minimize water spillage on floors, and moisture sensors in Equinix data centers. The OA will ensure that the CA and CSA records are protected from water exposure.

In addition, the Issuing CAs will rely on the default physical controls to mitigate risks with water exposure threats.

5.1.5 Fire Prevention and Protection

The OA has contracted with Equinix to provide non-water-based fire prevention and protection mechanisms for the physical hardware for CA systems.

5.1.6 Media Storage

The CA will protect media from unauthorized access, accidental damage, and environmental hazards.

5.1.7 Waste Disposal

The OA will destroy digital media in a manner to ensure the information is unrecoverable prior to disposal. If the digital media is destroyed by third-party vendors (, the OA will receive Certificate of Destruction (CoD) from the vendors. Further, the Issuing CAs shred paper media to prevent recovering the sensitive information.

5.1.8 Off-Site Backup

The OA leverages a hybrid environment with virtual and physical infrastructure.

5.2 PROCEDURAL CONTROLS

5.2.1 Corporate Controls

No Stipulation.

5.2.2 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles will be extraordinarily responsible to ensure the integrity of the CA is not weakened.

5.2.2.1 CA Systems Administrator

The CA System administrator is responsible for:

- Installation, configuration, and maintenance of the CA.
- Establishing and maintaining CA system accounts.
- Configuring Certificate profiles or templates and Audit parameters, and
- Generating and backing up CA keys.
- CA System Administrators do not issue Certificates to Subscribers.

5.2.2.2 Audit Administrator or Auditor

The auditor's role is responsible for:

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

5.2.2.3 CA Operator

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

5.2.2.4 Registration Authority

The Registration Authority is 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.

5.2.2.5 CSA Roles

The Certificate Status Authority (CSA) role encompasses the following responsibilities:

A CSA has the following roles:

The CSA Administrator is responsible for:

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

The CSA Auditor is responsible for:

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

The CSA Operator is responsible for:

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

5.2.2.6 Device Sponsor

A Device Sponsor serves as a proxy for non-human system components, like routers and firewalls, that are identified as subjects in Public Key Certificates. Collaborating with Registration Authorities (RAs), the Device Sponsor oversees the registration of these components. Their responsibility includes fulfilling the obligations specified for Subscribers in the CP and this document.

Device Sponsors hold a credential that is of equal or greater Assurance Level than the credential they are sponsoring.

5.2.2.7 Trusted Agent

NPE-IDMS Trusted Agents hold the responsibilities of:

- Validating identities, and
- Safely transmitting Subscriber information to the Registration Authority (RA).

5.2.2.8 Role Sponsor

Not applicable.

5.2.3 Number of Persons Required per Task

The OA will adhere to principles of duty separation and least privilege, ensuring no single individual can compromise the confidentiality, integrity, or availability of CA, RA, and CSA systems; repositories; and archives. Trusted Roles are only assigned operations in accordance with least privilege principles.

Notably, two-person controls are mandatory for several operations.

5.2.4 Identification and Authentication for Each Role

Persons in Trusted Roles are identified, authenticated, and authorized.

5.2.5 Roles Requiring Separation of Duties

The OA implements the following principles of duty separation for Trusted Roles:

5.3 PERSONNEL CONTROLS

5.3.1 Background, Qualifications, Experience, & Clearance Requirements

The OA will maintain controls to ensure that its personnel and employment practices augment the trustworthiness of its operations.

The OA will ensure that its personnel, including employees and contractors, are equipped with the necessary skills, knowledge, and experience for their respective job functions.

5.3.2 Background Check Procedures

The OA will require personnel assigned to Trusted Roles to have a FAA PIV credential, which means the personnel will have already had a Background Check.

5.3.3 Trusted Role

Personnel serving in a Trusted Role will have an active PIV card that was issued by the FAA, as stated in 5.3.1 above. Failure to timely renew the PIV card will result in the loss of the Trusted Role access to the CA.

5.3.4 Training Requirements

The Issuing CAs will provide training to personnel in Trusted Roles that includes the following topics:

- Security awareness
- Basic PKI concepts.
- CA/B Forum requirements.
- CA, RA, and CSA system versions.
- CA and RA security principles and mechanisms.

Role specific policies and procedures including business continuity and disaster recovery.

5.3.5 Retraining Frequency and Requirements

The OA reviews the topics and updates the training for personnel in Trusted Roles at least annually. Moreover, the Issuing CAs require annual (one per year) security awareness training for all personnel.

5.3.6 Job Rotation Frequency and Sequence

No stipulation.

5.3.7 Corrective Action for Unauthorized Actions

The Issuing CAs will take appropriate disciplinary actions, up to and including termination when personnel or contractors from third-party vendors have performed actions not authorized in the CPS.

5.3.8 Independent Contractor Requirements

The OA will hold third-party contractors to the personnel requirements in this CPS Section 5.3 as applicable.

5.3.9 Documentation Supplied To Personnel

The OA will provide personnel in Trusted Roles with the documentation required to perform their duties. This will include applicable portions of the CP and CPS, relevant law, regulation, policy and contracts, and other technical, operations and administrative documents.

5.4 AUDIT LOGGING PROCEDURES

5.4.1 Types of Events Recorded

Types of Events Recorded

At a minimum, each audit record will 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 Issuing CAs have implemented a program to detect and report security events for physical and virtual infrastructure; HSMs; and CA, RA, and CSA systems. The Issuing CAs record the following security events:

HSM Events

- HSM receipt and installation.
- HSM removal from and return to storage.
- HSM activation and usage.
- HSM zeroization.
- Decision to repair or retire HSM.

Certificate Application Events

- Identification method applied and information used to meet Subscriber requirements.
- Record of unique identification data, numbers, or combination thereof from identity documents.
- Storage location of Certificate Application and identity documents.
- Identity of Organization accepting Certificate Applications.
- Method used to validate identity documents.
- Acceptance of Certificate Request Workflows by Applicants.
- Consent by Subscriber allowing Issuing CAs to collect, store, and process personal data .

CA Certificate Events

- All key-related operations for CA Certificates including generation, storage, recovery, back up, transportation, migration, archival, and destruction.
- Identity of users authorizing key-related operations.
- Identity of users handling of Key Pairs for CA Certificates or key-related materials
- Identity of users having custody and handling of key-related materials and/or Key Pairs for CA Certificates.
- Compromise of Private Keys for CA Certificates.
- Decision to retire Key Pairs for CA Certificates.

End Entity Certificate Events

- All key-related operations for End Entity Certificates including generation, distribution, back up, escrow, storage, recovery, archival, and destruction.
- Certificate Requests for initial, renewals, and rekeys.
- Submission of Public Keys of End Entity Certificates
- Revocation and Suspension Requests
- Approvals and rejections of Certificate and Revocation Requests
- Issuance, revocation, suspension, and reactivation of End Entity Certificates
- Generation and issuance of CRLs and OCSP Responses
- Changes of Organization affiliation for End Entity Certificates
- Identity of users authorizing key-related operations
- Compromise of Private Keys for End Entity Certificates
- Violations of the CP and CPS

Security Events

- Security-sensitive files or records read or written including audit logs.
- Actions taken against security-sensitive data.
- Secure profile changes.
- Success and failures of identification and authentication mechanisms.
- System crashes, hardware failures, and other anomalies.
- Actions taken by personnel assigned to Trusted Roles.
- Changes of Organization affiliation for personnel.
- Decisions to bypass encryption and/or authentication mechanisms.
- Access to CA system or components thereof.
- Changes to operating system clocks or network time protocols.
- Electrical Power Outages, Uninterruptible Power Supply (UPS) failure
- Resetting operating system clock

Additionally, the Issuing CAs will include the following information automatically or manually for each security event:

- Event type.
- Entry unique identifier.
- Entry date and time.
- Entry source.
- User or system generating event.
- Success or failure indicator (if applicable).

5.4.2 Frequency of Processing Log

The Issuing CAs systematically process audit logs on a daily basis. These will be logs are gathered automatically from a range of sources, including the physical infrastructure, virtual infrastructure, HSMs, and systems for the CA, RA, and VA.

5.4.3 Retention Period for Audit Logs

The OA will hold onto the audit logs on-site for at least sixty (60) days, or beyond if the review process extends past this period.

5.4.4 Protection of Audit Logs

The Issuing CAs retain copies of the audit logs for at least thirty (30) days. In addition, the Issuing CAs archive the audit logs for at least two (2) years after the expiration of the End Entity Certificates.

For *Medium* assurance or Higher, system configuration and procedures will 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).
- There remains perpetual continuity of audit logs.
- Only authorized people may archive audit logs.
- Audit logs are not modified.

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

5.4.5 Audit Log Backup Procedures

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

5.4.6 Audit Collection System (internal vs. external)

The OA employs an external audit system for the management of audit logs.

5.4.7 Notification to Event-Causing Subject

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

5.4.8 Vulnerability Assessments

On a quarterly basis, the OA conducts vulnerability assessments on both the physical and virtual infrastructure. This involves identifying any foreseeable internal and external threats that could impact the confidentiality, integrity, or availability of the CA, RA, and CSA systems.

5.5 RECORDS ARCHIVE

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

5.5.1 Types of Events Archived

The Issuing CAs will archive the following records:

- Certificate and Public Keys
- **PKI Documentation**
  - CP and CP versions
  - Certificate Request Workflows versions
  - Trusted Role Charter versions
  - Trusted Role assignments and acknowledgements
  - Risk assessments and registers
  - PMA meeting minutes
  - Contracts with third-party vendors related to CA, RA, or CSA systems
  - Key ceremony authorization, logs, scripts, and videos
  - Security accreditations
  - Compliance Auditor reports, both internal and external
  - Documentation required by Compliance Auditors
  - Certificate problem reports
  - CP and CPS violations
  - Audit Logs
  - HSM Events
  - Certificate Application Events
  - CA Certificate Events
  - End Entity Certificate Events

5.5.2 Retention Period for Archive

The OA will retain the records for ten (10) years and six (6) months.

5.5.3 Protection of Archive

The OA will safeguard the confidentiality, integrity, and availability of the archive.

5.5.4 Archive Backup Procedures

The OA uses the archive which securely backs up the archive.

5.5.5 Requirements for Time-Stamping of Records

The OA will ensure timestamps records in the archive in accordance with this CPS Section 6.8.

5.5.6 Archive Collection System (Internal or External)

No stipulation.

5.5.7 Procedures to Obtain and Verify Archive Information

The OA has produced the Archive procedure that documents steps required to retrieve and verify records.

5.6 KEY CHANGEOVER

To minimize the Risk from Compromise of a CA's private signing key, the OA will the OA will change Public/Private Key Pairs for CA and End Entity Certificates based on the maximum Private Key usage period as specified in this CPS Section 6.3.2. Further, the OA may modify certificate profiles and Subject DN information to adhere to new best practices. Moreover, the OS retain the Private Keys for CA Certificates through the expiration of all End Entity Certificates issued by those CA Certificates.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

If a CA or CSA detects a potential penetration or other form of Compromise, it will 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 5.7.3 will be followed. Otherwise, the damage will be assessed to determine if the remediation required will 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 required based on a risk assessment, duress alarms will be provided for users who might be the target of coercion.

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

When CA or CSA computing resources, software, and/or data are damaged, rendered inoperative or

5.7.3 Private Key Compromise Procedures

The OA will immediately follow the incident response plan to investigate all incidents about lost, destruction, and suspected compromises of the Private Keys for CA Certificates.

5.7.4 Business Continuity Capabilities after a Disaster

The OA will define disaster recovery procedures in the business continuity plan for CA, RA, and CSA systems. In the event of a disaster, the OA will give priority to CSA systems to generate and publish status information about CA and End Entity Certificates.

5.8 CA, CSA, STP OR RA TERMINATION

Per the Business Continuity Plan the OA will promptly notify Customers, Subscribers, Device Sponsors, Relying Parties, Regulatory Authorities, and Organizations with Cross Certificates about the cessation of operations.

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

All cryptographic key material is generated using approved methods based on United States Federal Information Processing Standard (FIPS) standard.

The OA and Subscribers generate the Public and Private Keys in Cryptographic Modules for the different types of Certificates based on the following table:

Role / Certificate Profile	FIPS 140-2 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
MediumTSP	2	Hardware	Yes
MediumHardwareDevice	2	Hardware	Yes, for all Certificate profiles except for Subscriber Encryption
MediumDevice	1	Software	No
LowTSP	No requirements	Software /Hardware	No
LowDevice	See section 6.2.1.1 Custodial Key Stores	Software /Hardware	No

Random numbers will be generated within FIPS 140-2 or later 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 will 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.

6.1.2 Private Key Delivery to Subscriber

For CA Certificates, the OA creates the Public and Private Keys in Cryptographic Modules. Since the Private Keys do not leave the Cryptographic Modules, there is no Private Key delivery.

Refer to:

- CPS Section 6.1.1.3 Key Pair Generation (Subscriber Certificates)

6.1.3 Public Key Delivery to Certificate Issuer

For CA Certificates, the OA will use CA software that directly communicates with the Cryptographic Modules to generate the Public and Private Keys.

For TLS and Digital Signature Certificates, the Device Sponsor will submit Certificate Request Form to the RA software which will verify proof-of-possession as defined in Section 3.2.1

The sponsor, upon submitting a certificate signing request (CSR), initiates the generation of a private key. The CA, in turn, confirms the sponsor's control over the private key and then proceeds

to deliver through the FAA Email secure workflow the corresponding public key back to the sponsor.

Refer to:

- Section 3.2.1 Method to Prove Possession of Private Keys

6.1.4 CA Public Key Delivery to Relying Parties

For every CA public key issued, whether self-signed or otherwise, a cryptographic has of the key will be generated using a secure hash algorithm (e.g., SHA-256 or higher).

The OA will distribute the Public Keys of CA Certificates in the following secure manners to preclude substitution attacks.

6.1.5 Key Sizes

The OA will configure certificate profiles for CA and Subscriber Certificates in the CA software to require the minimum 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 OA will enable cryptographic network protocols in the production environments to meet the above minimum key sizes and algorithms.

Further, the OA will configure the CA software to use the following minimum hashing algorithms for Certificates, CRLs, and OCSP Responses:

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

Additionally, the OA configures CRLS and OCSP Responses in the CA software to use the same or better signature algorithms, key sizes, and hash algorithms used for the Certificates being validated.

Finally, the PMA requires OA to revoke affected Certificates if the security of a signing or hashing algorithm becomes compromised in accordance with Section 9.17.2.

Refer to:

- NIST 800-56A Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography

6.1.6 Public Key Parameters Generation and Quality Checking

The OA will configure the CA software and HSMs to generate Public Keys, Private Keys, and Prime Numbers in accordance with the FIPS 186-5 or higher standard.

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

The OA will configure the Key Usage extension in the certificate profiles of the CA software to bind the Public Keys to either signature or encryption, but not both except as specified in the following table:

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

If the Certificates will be used for authentication of ephemeral keys, the OA will configure the certificate profiles in the CA software to assert digitalSignature and/or nonRepudiation bits in the Key Usage extension. The OA may or may not assert keyEncryption and keyAgreement depending on the Public Key in the Certificate.

The OA will ensure the extended key usage OIDs are consistent with the key usage bits set.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

The relevant standard for Cryptographic Modules 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. The OA and Subscribers will utilize Cryptographic Modules validated with FIPS 140-2 Level or later standard, as outlined in this CPS Section 6.1.1. The PMA will have the right to review technical documentation related to any Cryptographic Modules being evaluated for use by Certificate Authorities (CAs). This right will be exercised by notifying the OA.

6.2.1.1 Custodial Subscriber Key Stores

The OA will use Cryptographic Modules with a minimum rating of FIPS 140-2 Level 2 or later to safeguard the Private Keys for OCSP Responder Certificates.

Subscribers Certificates contained in cryptographic modules used for custodial subscriber keys stores have varying requirements depending on the assurance level of their Subscriber Certificates. For LowDevice or LowTSP assurance levels, Subscribers can use Cryptographic Modules with a rating of FIPS 140-2 Level 1 or later to protect their Private Keys. However, for Subscriber Certificates at MediumDevice, MediumHardwareDevice, or MediumTSP assurance levels, Subscribers must employ Cryptographic Modules with a minimum rating of FIPS 140-2 Level 2 or later.

In situations where Certificates of Low and Medium assurance levels are stored in the same Cryptographic Modules, Subscribers are obligated to use Cryptographic Modules with a minimum rating of FIPS 140-2 Level 2 or later.

Refer to:

- CPS Section 6.1.1 Key Pair Generation

6.2.2 Private Key Multi-Person Control

Use of a CA private signing key will be under multiple person control as provided in 5.2.3

6.2.3 Private Key Escrow

The OA will not escrow the Private Keys associated with the Certificate Authority (CA), Transport Layer Security (TLS), Digital Signature, and Online Certificate Status Protocol (OCSP) Responder Certificates.

6.2.4 Private Key Backup

6.2.4.1 Backup of CA Private Signature Key

The OA will back up the Private Keys for CA OCSP Responder Certificates. These backups will be conducted under multi-person control.

6.2.4.2 Backup of Subscriber Private Signature key

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

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

6.2.4.3 Backup of CSA Subscriber Key Management Private Keys

Not applicable.

6.2.4.4 Backup of CSA Private Key

The OA are not required to back up the Private Keys for OCSP Responder Certificates. In case of a key loss or compromise, instead of restoring the Private Keys, OA revokes the existing certificate and request new OCSP Responder Certificates, following the guidelines outlined in this CPS Sections 4.3 and 4.9.

Refer to:

- CPS Section 4.3 Certificate Issuance
- CPS Section 4.9 Certificate Revocation

6.2.4.5 Backup of High-ContentSigning Key

Not applicable.

6.2.4.6 Backup of NPE Private Keys

Device Sponsor are not required to back up Private Keys for Subscriber Certificates at Low or Medium assurance levels. In the event of key loss or compromise, instead of restoring the Private Keys, Subscribers follow the procedure outlined in this CPS Sections 4.3 and 4.9. This procedure involves the revocation of the compromised certificate and the request for issuance of new Subscriber Certificates.

Refer to:

- CPS Section 4.3 Certificate Issuance
- CPS Section 4.9 Certificate Revocation

6.2.5 Private Key Archival

The OA do not archive the Private Keys for CA Certificates.

6.2.6 Private Key Transfer into or from a Cryptographic Module

The OA export the Private Keys for CA and OCSP Responder Certificates solely from the hardware-based Cryptographic Modules, and this is done in line with the key backup procedures detailed in this CPS Section 6.2.4. The OA also ensures that these Private Keys never exist in unencrypted form outside of the hardware-based Cryptographic Modules.

6.2.7 Private Key Storage on Cryptographic Module

The OA and Device Sponsors keep the Private Keys within FIPS 140-2 Cryptographic Modules, adhering to the guidelines specified in this CPS Section 6.1.1.

6.2.8 Method of Activating Private Keys

For Cryptographic Modules rated at FIPS 140-2 Level 3, which contain the Private Keys for Certificate Authority (CA), the OA establishes a multi-factor access configuration (m of n) with a minimum requirement of 2 out of 10 authorized individuals.

Device Sponsor authenticates using PIV and decrypts the activation code using their FAA PIV.

6.2.9 Methods of Deactivating Private Keys

Cryptographic Modules that have been activated is not available to unauthorized access, see section 6.2.1. Cryptographic Module Standards and Controls.

If the online cryptographic module is inactivity for a period of inactivity, the cryptographic module is deactivated. The cryptographic module is securely housed in the IDMS Rack.

Private Keys do not leave the cryptographic module.

6.2.10 Method of Destroying Private Keys

For the CA and OCSP Responder Certificates, the OA leverages multi-person control to input the zeroize command in the hardware-based Cryptographic Modules, thereby destroying the Private Keys. Physical destruction of hardware-based Cryptographic Modules is not part of this process.

6.2.11 Cryptographic Module Rating

The OA and Subscribers use Cryptographic Modules as defined in Section 6.2.1.

6.3 OTHER ASPECTS OF KEY MANAGEMENT

6.3.1 Public Key Archival

The OA archives the Public Keys. All NPE-IDMS repositories are safeguarded, and public-facing repositories serve as read-only proxies that mirror data stored securely behind advanced firewall protections and archived daily.

Refer to:

- Section 5.5.1 Types of Events Archived.

6.3.2 Certificate Operational Periods/Key Usage Periods

The OA changes the Private Keys for CA and Device Certificates to minimize the risk of Key Compromise based on the following schedule as specified in this CPS Section 5.6:

Table X, Key Usage Periods:

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 CA	10 years	13 years	10 years	13 years	10 years	13 years
Issuing CA	10 years	13 years	10 years	13 years	10 years	13 years
Device Identity	3 years	≤ 3 years	3 years	≤ 3 years	3 years	≤ 3 years
Ground Device Identity for ATN/IPS	3 years	≤ 3 years	3 years	≤ 3 years	3 years	≤ 3 years
Device Signature	3 years	≤ 3 years	3 years	≤ 3 years	3 years	≤ 3 years
Device 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

The CA software does not generate Certificates with validity time periods longer than the CA Certificates.

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

Not applicable.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

The OA and Device Sponsor both adhere to secure practices when generating and managing activation data to safeguard Private Keys.

See Section 6.1.2 Private Key Delivery to Subscriber for activation data controls.

6.4.2 Activation Data Protection

See Section 6.1.2 Private Key Delivery to Subscriber for activation data protection.

6.4.3 Other Aspects of Activation Data

The OA changes the activation data for CA and OCSP Responder Certificates when a rekey occurs.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

The OA configure the CA systems to meet the following security requirements:

- Validate identity of users
- Assign users to roles based on least privilege required to perform job functions.
- Have strong password and session time out policies.
- Provision credentials and authenticators to users unique to CA systems.
- Require multi-factor authentication for users to login.
- Generate and archive audit records for all transactions.
- Enforce domain isolation and partitioning for security critical processes.
- Use cryptography to protect session communications.
- Ensure software and firmware integrity.
- Protect from malicious code and intrusion attacks.
- Support recovery from key or system failure.

The OA configure the RA systems to meet the following security requirements:

- Validate identity of users.
- Assign users to roles based on least privilege required to perform job functions.
- Have strong password and session time out policies.
- Provision credentials and authenticators to users unique to RA systems.
- Require multi-factor authentication for users to login.
- Communicate with CA systems through defined processes.
- Protect from malicious code and intrusion attacks.
- Support recovery from key or system failure.

The OA configure the CSA systems to meet the following security requirements:

- Validate identity of users.
- Assign users to roles based on least privilege required to perform job functions.
- Have strong password and session time out policies.

- Provision credentials and authenticators to users unique to CSA systems.
- Require multi-factor authentication for users to login.
- Communicate with CA systems through defined processes.
- Protect from malicious code and intrusion attacks.
- Support recovery from key or system failure.

6.5.2 Computer Security Rating

No stipulation.

6.6 LIFE-CYCLE (TECHNICAL) SECURITY CONTROLS

6.6.1 System Development Controls

The Software Development Engineers adhere to the following system development prerequisites for CA, RA, and CSA systems:

- Commercial, custom, and open-source software undergo design, development, and testing phases under a structured and documented software development life cycle (SDLC) methodology.
- Hardware elements like servers and HSMs are procured via secure channels, ensuring a continuous accountability chain and mitigating tampering risks.
- Software downloads are obtained exclusively from authorized sources, with authenticity checks in place.
- All hardware, software, and virtual infrastructure undergo an initial and periodic vulnerability and malicious code scan.
- The issuance of an unauthorized certificate from any CA will be detected within 30 minutes.

6.6.2 Security Management Controls

The configuration of the CA, CSA equipment as well as any modifications and upgrades will be documented and controlled. There will 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 will be used for installation and ongoing maintenance of the CA, and CSA equipment. The CA and CSA software, when first loaded, will be verified as being supplied from the vendor, with no modifications, and be the version intended for use.

The OA adhere to the following system configuration guidelines for the CA, RA, and CSA systems:

- A structured and documented system configuration methodology is established for controlling, monitoring, and maintaining the CA, RA, and CSA system installations and configurations.
- A formal change management methodology is put in place for reviewing, testing, and authorizing alterations to existing system configurations, encompassing software releases, access control updates, and hardware deployments.
- Software used is verified to be the correct version from authorized vendors and free of modifications.
- Systems are designed to detect unauthorized modifications to existing configurations.

Finally, formal management responsibilities and procedures are in place to regulate changes to equipment, software, and operational procedures.

6.6.3 Life Cycle Security Ratings

The OA adheres to the FAA System Acquisition Policy for the procurement and installation of hardware and software via authorized contractual mechanisms. In addition, they have established Operational Policy that guides updates to hardware, software, and firmware.

6.7 NETWORK SECURITY CONTROLS

Root CAs and their internal PKI repositories are offline.

The OA implements the following network security measures for the CA, RA, and CSA systems:

- Denial of service and intrusion attacks are mitigated with a range of controls including security guards, firewall rules, and an intrusion detection/prevention system.
- Boundary control devices restrict all but essential network services.
- Unused network ports and services are deactivated.

6.8 TIME STAMPING

The OA implements the following time stamping procedures for the CA, RA, and CSA systems:

- The systems are regularly synchronized (within 3 minutes) with a reliable and independent time service, using FAA NTP.
- A comprehensive and formalized procedure is in place for manually adjusting clocks on hardware, including HSMs and laptops.
- Records of these manual clock adjustments are diligently kept and routinely reviewed.

7. CERTIFICATE, CRL AND OSCP

7.1 CERTIFICATE PROFILE

7.1.1 Version Numbers

The OA configure certificate profiles in the CA software for issuing CA and End Entity Certificates, with the Version field designated as "2".

7.1.2 Certificate Extensions

Interoperability testing is completed by testing a representative set of end user applications for successful Certificate usage.

Critical private extensions are interoperable in the FAA community of use.

Issuer CA and Device Certificates includes extensions per the document Non-Person Identity (NPE) Certification Profiles addendum to the CP and CPS.

The OA configure certificate profiles in the CA software to include extensions within Certificates in accordance with RFC 5280, CA/B Forum Baseline Requirements, CA/B Forum EV Guidelines, and CA/B Forum Code Signing Baseline Requirements. Any optional or additional extensions are marked as “Non-Critical” and do not conflict with the Certificate and CRL profiles in the CP and this CPS which includes:

- Certificates do not have critical private extensions
- Certificates include the ExtendedKeyUsage (EKU) extension, but do not have “anyEKU” value
- CA Certificates do not include the “id-kp-serverAuth”, “id-kp-emailProtection”, “id-kp-codeSigning” or “id-kp-timeStamping” values in the same Certificate

7.1.3 Algorithm Object Identifiers

The OA configure certificate profiles in the CA software to limit the signature algorithms based on one (1) of the following OIDs from the SHA-2 family:

Certificate Name	OID
SHA256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
ecdsa-with-SHA384	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 3 }

The OA configure certificate profiles in the CA software to limit the cryptographic algorithm associated with the Subject Public Key in Certificates based on one (1) of the following OIDs:

Cryptographic Algorithm	OID
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 }

The OA configures certificate profiles in the CA software to prohibit issuing TLS Certificates with a Reserved IP Address or Internal Name.

7.1.4 Name Forms

The OA configure certificate profiles in the CA software to populate the Subject and Issuer DNs of Certificates with X.500 Distinguished Names that are composed of standard attributes found in RFC 5280.

7.1.4.1 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
	Recommended	OU	0..1	"Certification Authorities" or similar text
	Required	O	1	Issuer name, e.g., "O=XYZ Inc"
	Required unless entity is a multi-national organization	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.

7.1.4.2 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)

3684

7.1.4.3 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 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)

Every attribute in the DN is only allowed to have one attribute value.

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

7.1.5 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.

7.1.5.1 TLS Technically Constricted CAs

If the technically constrained CA Certificates have "id-kp-serverAuth" in the EKU extension, the OA configure certificate profiles in the CA software to add the Name Constraints extension with dNSName and iPAddress constraints.

Refer to:

- CPS Section 3.2.2 Authentication of Organization and Domain/Email Control

7.1.6 Certificate Policy Object Identifier

Except for Self-Signed Root CA, all CA and Subscriber Certificates issued under the CP and this CPS 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 assert all policy OIDs corresponding to the lower Assurance Levels defined in the CP and CPS.

Organizational Code-Signing and Role Based Code-Signing Certificates are Not applicable.

The OA configure certificate profiles in the CA software to assert one (1) or more of the following FAA and CA/B Forum Certificate OIDs in CA and End Entity Certificates, except for self-signed Root CA Certificates:

Digitally Signed Object	Object Identifier (OID)	CAB/Forum OID
Policy Documents	2.16.840.1.114412.0	
FAA Certificate Policy	<To be registered by FAA>	-
TLS Certificate	**<To be registered by FAA>**	**-**
Domain Validation TLS Certificate	<To be registered by FAA>	2.23.140.1.2.1
Organization Validation TLS Certificate	<To be registered by FAA>	2.23.140.1.2.2

7.1.7 Usage of Policy Constraints Extension

The OA configures the CA software, so Device Certificates assert the policy constraints extensions to inhibit policy mapping.

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

.

7.1.8 Policy Qualifiers Syntax and Semantics

The OA configure certificate profiles in the CA software to include this CPS URI in the Certificate Policies extension for CA and End Entity Certificates.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

No stipulation.

7.2 CRL PROFILE

7.2.1 Version Numbers

The OA configure CRL profiles in the CA software to issue CRLs with “1” in the Version field.

Refer to:

- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

7.2.2 CRL Entry Extensions

The OA do not configure CRL profiles in the CA software with CRL extensions.

7.3 OCSP PROFILE

The OA configure OCSP in the CA software which is based on RFC 6960.

7.3.1 Version Number

The OA configures the OCSP in the CA software to accept RFC 6960 Version 1 (v1) OCSP Requests and issue RFC 6960 v1 OCSP Responses.

7.3.2 OCSP Extensions

The OA configure OCSP in the CSA software to support the Nonce extension in OCSP Requests and OCSP Responses.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Both internal and external Auditors are engaged to ensure that the requirements of the CP and this CPS and the provisions of the contracts with cross-certified CAs are implemented and enforced.

CAs will 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 will require that Relying Parties acknowledge that their practices will fully comply with this CP.

Acknowledgements and Agreements will ensure persons and Entities understand that to falsely claim compliance with this CP, and such claims may give rise to legal actions against persons or Entities disregarding this prohibition.

CAs Internal Security assessments will be conducted annually on the PKI infrastructure as required by Agency policy.

8.1 FREQUENCY OF AUDIT OR ASSESSMENTS

The PMA will engage a qualified, independent Auditor to annually (one per year) evaluate the compliance of all PKI functions (e.g., CAs, RAs, etc.) with the CP and CPS.

8.2 IDENTITY AND QUALIFICATIONS OF ASSESSOR

The Auditor is accredited as:

- have qualifications in accordance with the best commercial practice and as mandated by law or appropriate regulatory agency or board.
- be a PECB certified ISO/IEC27001 lead auditor 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 and 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 (one per year) ongoing business activity [its primary responsibility].

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The compliance auditor will either represents a firm which is independent from the FAA being audited, or it will be sufficiently organizationally separated from the FAA to provide an unbiased, independent evaluation. 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 will be responsible for determining whether the compliance auditor meets the required criteria for independence.

8.4 TOPICS COVERED BY ASSESSMENT

The Auditor will verify that the FAA is complying with the requirements of the applicable CP, CPS (and any other applicable agreement that governs the FAA PKI). The Compliance Audit will also include a compliance analysis assessment that determines whether this CPS adequately addresses and implements the requirements of the applicable CP.

If the auditor uses statistical samplings, all PKI components and personnel, including PKI component managers and operators will be considered in the sample. The sample will vary on an annual (one per year) basis.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

For the CA, 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 will be performed.

8.5.1 PMA Notification

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

8.5.2 Remedy

If the PMA determines that a CA is not meeting its obligations outlined in the CP, this CPS with cross-certified PKIs, the PMA will take appropriate actions, including the suspension of operations or revocation of the CA certificate, development of a remediation plan and implementation of corrective actions within timeframes established by the PMA The following process will be followed to remedy a deficiency:

When the compliance auditor identifies a discrepancy between the CA design, operation or maintenance, and the stipulations of the CA CP, this CPS or the applicable documents.

8.5.3 Remedy by other CAs

The procedure for handling remedies for Certifying CAs will follow the following steps:

- Identification of Deficiency by the compliance auditor: Detect and identify the deficiency within the operations of a Certifying CA.
- Immediate Revocation: If the deficiency is critical and poses a significant security risk, as determined by the PMA in consultation with the OA, immediately revoke the Cross-Certification Certificates of the deficient CA.
- Allowance for Correction: If the deficiency is less critical, allow the deficient CA to continue operation for a period of ninety (90) days to correct the identified problems. After this period, review the corrections made. If the deficiency persists, proceed with the revocation of the Cross-Certification Certificates.
- Deferral of Action: If the deficiency is minor and does not immediately threaten the security or the operation of the network as determined by the PMA in consultation with the OA, note the irregularities and allow the deficient CA to continue operations. However, no

revocation should be done until the next scheduled audit. During this audit, revisit the noted deficiencies and assess whether they have been addressed. Proceed with revocation if deficiencies remain unaddressed.

8.5.4 Factors Considered

The PMA and OA will follow the following procedure for decision making regarding deficient actions:

- Problem Analysis: The OA will begin with a comprehensive analysis of the identified deficiency, examining the nature and implications of the problem.
- Review of Past Responses: The OA will look at how similar issues have been handled in the past. Assess the effectiveness of those responses and whether they could be applied in the current situation.
- Assessment of Severity and Risk: The OA will evaluate the severity of the deficiency and the risk it imposes on the system or community. Consider the potential disruption that might be caused if certain actions are taken to address the deficiency.
- Notify the PMA: The OA will notify the PMA Chair of the deficiency and the OAs assessment of the risk.
- Special PMA meeting: The PMA Chair will schedule a special PMA meeting to allow the OA to report findings and assessment.
- Consider Auditor's Recommendations: The PMA, in consultation with the OA will review the recommendations made by the auditor regarding the deficiency. The auditor's professional judgment and expertise should significantly inform the decision-making process.
- Decision Making: Based on the above assessments, the PMA will make a decision about the appropriate course of action to take. This could range from immediate remediation efforts to a more long-term plan depending on the severity and impact of the deficiency.
- Implementation and Monitoring: Once a decision is made, the OA will implement the chosen course of action promptly and monitor its effectiveness closely. Modify the approach if it does not yield expected results or if the situation changes.
- Report to the PMA: The OA will inform the PMA Chair once the chosen course of action has been implemented and/or if modification of the approach is required.
- PMA meeting: The PMA Chair will invite the OA to the next PMA meeting (which may be a special meeting) to report on the completion of the remediation plan or to discuss and get approval for any modification.

8.5.5 Cross-Certification

The OA will follow the steps in the procedure for handling cross-certificate revocation.

- Receipt of Revocation Notification: Once a notification of cross-certificate revocation is received from another CA, ensure all details are understood clearly.

- Update Authority Revocation List (ARL): Immediately update the ARL to reflect the received revocation. This step should be prioritized to maintain the security and integrity of the system.
- Communication with Subscribers: Prepare a clear and concise message to all subscribers informing them about the revocation. The message should contain details about the revoked cross-certificate and implications, if any.
- Notify Affiliated Organizations: Similarly, notify all affiliated organizations about the revocation. Ensure all key parties are informed promptly to maintain transparency.
- Outline Future Course of Action: In your communications to subscribers and affiliated organizations, also include information on how the situation will be handled moving forward. This could be steps taken to mitigate any risks or impacts, or procedures to replace the revoked cross-certificate.
- Implementation and Monitoring: Implement the outlined plan of action within the timeframe detailed in the remediation plan and monitor its effectiveness. If necessary, update your subscribers and affiliated organizations on any changes or updates in the plan.

8.6 COMMUNICATIONS OF RESULTS

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

8.6.1 Persons to be Notified

The OA will publish the final audit reports in Repositories no later than three (3) months after the end of the audit period.

The conclusive results of the audit will be directly communicated to the RA, the CA, all Cross-Certified CAs and stakeholders but will be summarized as require so as not expose the system to unnecessary risks no later than three (3) months after the end of the audit period.

If the OA will be unable to publish the final audit reports within this timeframe, the OA will provide bridge letters signed by the Auditor explaining the delays.

8.6.2 Communication of Remedy

Refer to CPS Section 8.5 and the first paragraph of 8.6.

8.6.3 Retention of Audit Report

The OA will archive the evidence and final audit reports and the data used as evidence to support the conclusions and findings for at least ten (10) years and six (6) months. The OA will retain the audit report and evidence for longer periods if required by law or regulation.

8.6.4 Self-Audits

The Issuer CA will have internal Audits performed by an independent Auditor at least once per year to assess compliance with the CP and this CPS. Further, the independent auditor will review at least three (3) percent of End Entity Certificates to verify the content matches the end entity and certificate profiles as well as the Certificate Requests.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 Certificate Issuance/Renewal Fees

No Stipulation.

9.1.2 Certificate Access Fees

No Stipulation.

9.1.3 Revocation or Status Information Access Fee

No Stipulation.

9.1.4 Fees for other Services

No Stipulation.

9.1.5 Refund Policy

No Stipulation.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

FAA CAs that need to contract or cross certify with Non-governmental Entities who are CAs, CMSs, CSSs, or RAs will 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.

9.2.2 Other Assets

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

9.2.3 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 will 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.

9.3.1 Information Not Within the Scope of Confidential Information

No Stipulation.

9.3.2 Responsibility to Protect Confidential Information)

No Stipulation.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 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

9.4.2 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.

9.4.3 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.

9.4.4 Responsibility to Protect Private Information

See Section 9.4.2.

9.4.5 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).

9.4.6 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.

9.4.7 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.

9.5.1 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.

9.5.2 Property Rights in the CPS

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

9.5.3 Property Rights in Names

No Stipulation.

9.5.4 Property Rights in Keys

No Stipulation.

9.6 REPRESENTATIONS AND WARRANTIES

No Stipulation.

9.6.1 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 CPS 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.

9.6.2 RA Representations and Warranties

No Stipulation.

9.6.3 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.

9.6.4 Relying Parties Representations and Warranties

No Stipulation.

9.6.5 Representations and Warranties of Affiliated Organizations

9.6.5.1 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

9.9.1 Indemnification by Entity CA

No Stipulation.

9.9.2 Indemnification by Relying Party

No Stipulation.

9.9.3 Indemnification by Subscribers

No Stipulation.

9.10 TERM AND TERMINATION

9.10.1 Term

The CP and this CPS has no specified term.

No Stipulation.

9.10.2 Termination

No Stipulation.

9.10.3 Effect of Termination and Survival

The following requirements of the CP and this CPS 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

9.12.1 Procedure for Amendment

The PMA will review the CP at least once every year.

The OA will review the CPS at least once every year.

The CPS and amendments to it will become effective once approved by the OA.

The CP and amendments to it shall become effective once approved by the PMA.

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

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

9.12.2 Notification Mechanism and Period

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

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

9.12.3 Circumstances under which OID must be changed

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

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

9.13 DISPUTE RESOLUTION PROVISIONS

No Stipulation.

9.13.1 Disputes among the PMA/OA and Third Parties

No Stipulation.

9.13.2 Alternate Dispute Resolution Provisions

No Stipulation.

9.14 GOVERNING LAW

This CPS 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 CPS will be governed by the federal law of the United States.

9.15 COMPLIANCE WITH APPLICABLE LAW

FAA and Entity CAs will comply with all applicable laws.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire agreement

No Stipulation.

9.16.2 Assignment

No Stipulation.

9.16.3 Severability

No Stipulation.

9.16.4 Enforcement (Attorney Fees/Waiver of Rights)

No Stipulation.

9.16.5 Force Majeure

No Stipulation.

9.17 OTHER PROVISIONS

9.17.1 Prohibited Certificate Uses

9.17.2 FAA will not use any Certificate for a prohibited purpose. Corporate Controls

No Stipulation.

9.17.3 Background, Qualifications, Experience, & Clearance Requirements

No Stipulation.

9.17.4 Background Check Procedures Adjudication

No Stipulation.

9.17.5 Retention Period for Archive

If the original media cannot retain the data for the required period, a mechanism to transfer the archived data to new media will 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

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

Certificates and CRLs issued under a policy OID of this CP will not contain any critical extensions not listed in the profiles in this section or in Section 7.1.2. Certificates and CRLs issued under a policy OID of this CP may contain non-critical extensions not listed in the profiles in this section provided interoperability is not affected.

CAs may issue partitioned CRLs according to the following criteria:

- The CRLs are not indirect CRLs
- The CRLs are not partitioned by reason code
- CRL Distribution Point and Issuing Distribution Point do not assert a name relative to the Issuer.

If the CA provides OCSP services, the CA will also issue a full and complete CRL (i.e., a CRL without an Issuing Distribution Point extension) for use by the OCSP responder.

10.1 PUBLIC ROOT CA CERTIFICATE PROFILE

Base Certificate	Value		
Cert Type	CA		
Cert Profile Name	ROOT CA		
Version	V3 (2)		
Serial Number	Generate a non-sequential number containing at 160 bits based on a cryptographically secure pseudorandom number generator (CSPNG)		
Issuer Signature Algorithm	SHA512WithRSAEncryption {1 2 840 113549 1 1 13}		
Issuer Distinguished Name	**Attribute**	**Attribute Value**	**Dictionary String 1**
	C	US	PrintableString
	O	Federal Aviation Administration	UTF8String
	CN	Common Name conforming to section 7.1.4.1 of the FAA NPE CP	UTF8String

Validity Period Not Before	ZZZZ/MM/DD HH:MM:SS Z **Note:** CA software uses the certificate generation date and time expressed in UTC Time during the key ceremony		
Validity Period Not After	ZZZZ/MM/DD HH:MM:SS Z **Note:** CA software uses the certificate generation date and time plus **20 years (7,306 days)** expressed in UTC Time		
Subject Distinguished Name	**Attribute**	**Attribute Value**	**Dictionary String 2**
	C	US	PrintableString
	O	Federal Aviation Administration	UTF8String
	CN	Common Name conforming to section 7.1.4.1 of the FAA NPE CP, identical to the CN of the Issuer Distinguished Name	UTF8String
Subject Public Key Info	4096-bit		
Signature Algorithm	SHA512WithRSAEncryption {1 2 840 113549 1 1 13}		
Certificate Extensions	Value		
Extension	**Criticality**	**Description**	
Subject Key Identifier	False	Octet String **Note:** CA software calculates a SHA-1 hash of the Subject Public for this certificate	
Key Usage	True	Key Certificate Signature	Enable
		CRL Signature	Enable
Basic Constraints	True	Certificate Authority	Enable
		Path Length Constraint	Absent

4148

4149

10.2 PUBLIC ISSUING CA CERTIFICATE PROFILE

Base Certificate	Value		
Cert Type	CA		
Cert Profile Name	ISSUING CA		
Version	V3 (2)		
Serial Number	Generate a non-sequential number containing 160 bits based on a cryptographically secure pseudorandom number generator (CSPNG)		
Issuer Signature Algorithm	SHA384WithRSAEncryption {1 2 840 113549 1 1 12}		
Issuer Distinguished Name	**Attribute**	**Attribute Value**	**Dictionary String 1**
	C	US	PrintableString
	O	Federal Aviation Administration	UTF8String
	CN	Identical to the Subject CN of the Issuing CA for this certificate.	UTF8String
Validity Period Not Before	ZZZZ/MM/DD HH:MM:SS Z **Note:** CA software uses the certificate generation date and time expressed in UTC Time during the key ceremony		
Validity Period Not After	ZZZZ/MM/DD HH:MM:SS Z **Note:** CA software uses the certificate generation date and time plus **10 years (3,653 days)** expressed in UTC Time		
Subject Distinguished Name	**Attribute**	**Attribute Value**	**Dictionary String 2**
	C	US	PrintableString
	O	Federal Aviation Administration	UTF8String
	CN	CN conforming to Section 7.1.4.1 of the FAA NPE CP	UTF8String
Subject Public Key Info	3072-bit		
Signature Algorithm	SHA384WithRSAEncryption {1 2 840 113549 1 1 12}		
Certificate Extensions	Value		
Extension	**Criticality**	**Description**	**Setting**

Authority Key Identifier	False	Octet String **Note:** CA software adds the Subject Key Identifier from the CA that issued this certificate	
Subject Key Identifier	False	Octet String **Note:** CA software calculates a SHA-1 hash of the Subject Public Key for this certificate	
Key Usage	True	Key Certificate Signature	Enable
		CRL Signature	Enable
		Digital Signature	Enable
Basic Constraints	True	CA	Enable
		Path Length Constraint	Absent
Certificate Policies	False	Policy Identifier	{2 23 140 1 2 1} Domain Validated
		Policy Identifier	{2 23 140 1 2 2} Organization Validated
		Policy Identifier	{1.3.27.16.1.1.0} ICAO Certificate Policy
		Policy Identifier	{1 3 6 1 4 1 44109 0 1} FAA NPE Certificate Policy CPS URI: FAA NPE CP file via a publicly available URL FAA External DNS
CRL Distribution Point	False	Distribution Point	Latest CRL file issued by FAA Root CA via a publicly available URL FAA External DNS
Authority Access Information	False	CA Issuer	FAA IDMS Root CA certificate via a publicly available URL FAA External DNS
Inhibit Policy Mapping	False	skipCertificates	0

4151

4152

4153

4154 10.3 INTERNAL ISSUING CA PROFILE

Base Certificate	Value		
Cert Type	CA		
Cert Profile Name	ISSUING CA		
Version	V3 (2)		
Serial Number	Generate a non-sequential number containing 64 bits based on a cryptographically secure pseudorandom number generator (CSPNG)		
Issuer Signature Algorithm	SHA512WithRSAEncryption {1 2 840 113549 1 1 13}		
Issuer Distinguished Name	**Attribute**	**Attribute Value**	**Dictionary String 1**
	C	US	PrintableString
	O	Federal Aviation Administration	UTF8String
	CN	Common Name of the signing CA for this certificate	UTF8String
Validity Period Not Before	ZZZZ/MM/DD HH:MM:SS Z **Note:** CA software uses the certificate generation date and time expressed in UTC Time during the key ceremony		
Validity Period Not After	ZZZZ/MM/DD HH:MM:SS Z **Note:** CA software uses the certificate generation date and time plus **10 years (3,653 days)** expressed in UTC Time		
Subject Distinguished Name	**Attribute**	**Attribute Value**	**Dictionary String 2**
	C	US	PrintableString
	O	Federal Aviation Administration	UTF8String
	CN	Common Name conforming to section 7.1.4.1 of the NPE Certificate Policy	UTF8String
Subject Public Key Info	3072-bit		
Signature Algorithm	SHA384WithRSAEncryption {1 2 840 113549 1 1 12}		

Certificate Extensions	Value		
Extension	**Criticality**	**Description**	**Setting**
Authority Key Identifier	False	Octet String **Note:** CA software adds the Subject Key Identifier from the CA that issued this certificate	
Subject Key Identifier	False	Octet String **Note:** CA software calculates a SHA-1 hash of the Subject Public Key for this certificate	
Key Usage	True	Key Certificate Signature	Enable
		CRL Signature	Enable
		Digital Signature	Enable
Extended Key Usage	False	Server Authentication	Enable
		Client Authentication	Enable
Basic Constraints	True	CA	Enable
CRL Distribution Point	False	Distribution Point	Latest CRL file issued by FAA IDMS Internal Root CA via an internal URL FAA Internal DNS
Authority Access Information	False	CA Issuer	FAA IDMS Internal Root CA certificate via an internal URL FAA Internal DNS

4155
4156

10.4 TLS SERVER AUTH CERT (FQDN) FOR RSA KEYS

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	SHA384WithRSAEncryption {1 2 840 113549 1 1 12}
Issuer Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4.1 of this CP, matching the Subject Distinguished name of the Issuing CA certificate.
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
Subject Public Key Information	2048, 3072, or 4096-bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11},
Extension	**Value**
Authority Key Identifier	c=no Octet String **Note:** CA software adds the Subject Key Identifier from the CA that issued this certificate
Subject Key Identifier	c=no Octet String **Note:** CA software calculates a SHA-1 hash of the Subject Public Key for this certificate
Key Usage	c=yes digitalSignature keyEncipherment
Extended Key Usage	c=no (Mandatory) id-kp-serverAuth {1 3 6 1 5 5 7 3 1} (Optional) id-kp-clientAuth {1 3 6 1 5 5 7 3 2}

Certificate Policies	c=no {2 23 140 1 2 2} Organization Validated {1 3 27 16 1 1 0} ICAO Certificate Policy {1 3 6 1 4 1 44109 0 1} FAA NPE Certificate Policy CPS URI:<FAA NPE CP file via a publicly available URL > Shall select one of the following OIDs based protection of private key or key usage for the end entity certificate: {1.3.27.16.1.1.0.2} LowDevice {1.3.27.16.1.1.0.3} Low-TSPMediatedSignature {1.3.27.16.1.1.0.5} MediumDevice {1.3.27.16.1.1.0.6} Medium-TSPMediatedSignature {1.3.27.16.1.1.0.8} MediumDeviceHardware
Subject Alternative Name	c=no; (Mandatory) Host URL | Host NameShall include one or more dNSName=additional name where “additional name” is per section 7.1.4
Authority Information Access	c=no FAA IDMS Issuing CA certificate via a publicly available URL OCSP Responder service for FAA IDMS Issuing CA via a publicly available URL
CRL Distribution Points	c = no; (Latest CRL file issued by FAA IDMS Issuing CA accessible via a publicly available URL
Embedded SCTs	c=no; (WebTrust Mandatory) This extension must appear in all TLS Server certificates issued by an Issuing CA participating in Web Browser Root Programs.

4159

4160

10.5 TLS SERVER AUTH CERT (FQDN) FOR ECC KEYS

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	SHA384WithRSAEncryption {1 2 840 113549 1 1 12}
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
Subject Public Key Information	256 bit prime, 233 bit binary, id-ecPublicKey {1 2 840 10045 2 1} or greater as specified in Section 6.1.5.
Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String **Note:** CA software adds the Subject Key Identifier from the CA that issued this certificate
Subject Key Identifier	c=no Octet String **Note:** CA software calculates a SHA-1 hash of the Subject Public Key for this certificate
Key Usage	c=yes; digitalSignature
Extended Key Usage	c=no (Mandatory)id-kp-serverAuth {1 3 6 1 5 5 7 3 1} (Optional) id-kp-clientAuth {1 3 6 1 5 5 7 3 2}

Certificate Policies	c=no {2 23 140 1 2 2} Organization Validated {1 3 27 16 1 1 0} ICAO Certificate Policy {1 3 6 1 4 1 44109 0 1} FAA NPE Certificate Policy CPS URI:< FAA NPE CP file via a publicly available URL > Shall select one of the following OIDs based protection of private key or key usage for the end entity certificate: {1.3.27.16.1.1.0.2} LowDevice {1.3.27.16.1.1.0.3} Low-TSPMediatedSignature {1.3.27.16.1.1.0.5} MediumDevice {1.3.27.16.1.1.0.6} Medium-TSPMediatedSignature {1.3.27.16.1.1.0.8} MediumDeviceHardware
Subject Alternative Name	c=no; (Mandatory) Host URL | | Host Name Shall include one or more dNSName=additional name where “additional name” is per section 7.1.4
Authority Information Access	c=no FAA IDMS Issuing CA certificate via a publicly available URL OCSP Responder service for FAA IDMS Issuing CA via a publicly available URL
CRL Distribution Points	c = no . Latest CRL file issued by FAA IDMS Issuing CA via publicly available URL
Embedded SCTs	c=no (WebTrust Mandatory) This extension must appear in all TLS Server certificates issued by an Issuing CA participating in Web Browser Root Programs.

4163

4164

10.6 TLS SERVER AUTH CERT (IP ADDRESS) FOR RSA KEYS

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	SHA384WithRSAEncryption {1 2 840 113549 1 1 12}
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
Subject Public Key Information	2048-bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String **Note:** CA software adds the Subject Key Identifier from the CA that issued this certificate
Subject Key Identifier	c=no Octet String **Note:** CA software calculates a SHA-1 hash of the Subject Public Key for this certificate
Key Usage	c=yes; digitalSignature keyEncipherment
Extended Key Usage	c=no (Mandatory)id-kp-serverAuth {1 3 6 1 5 5 7 3 1} (Optional)id-kp-clientAuth {1 3 6 1 5 5 7 3 2}

Certificate Policies	c=no {2 23 140 1 2 2} Organization Validated {1 3 27 16 1 1 0} ICAO Certificate Policy {1 3 6 1 4 1 44109 0 1} FAA NPE Certificate Policy CPS URI:<FAA NPE CP file via a publicly available URL > Shall select one of the following OIDs based protection of private key or key usage for the end entity certificate: {1.3.27.16.1.1.0.2} LowDevice {1.3.27.16.1.1.0.3} Low-TSPMediatedSignature {1.3.27.16.1.1.0.5} MediumDevice {1.3.27.16.1.1.0.6} Medium-TSPMediatedSignature {1.3.27.16.1.1.0.8} MediumDeviceHardware
Subject Alternative Name	c=no (Mandatory) **IP Address** Shall include one or more iPAddress=additional name where “additional name” is per section 7.1.4
Authority Information Access	c=no FAA IDMS Issuing CA certificate via a publicly available URL OCSP Responder service for FAA IDMS Issuing CA via a publicly available URL
CRL Distribution Points	c = no Latest CRL file published by FAA IDMS Issuing CA via a publicly available URL
Embedded SCTs	c=no (WebTrust Mandatory) This extension must appear in all TLS Server certificates issued by an Issuing CA participating in Web Browser Root Programs.

4168

4169

10.7 TLS SERVER AUTH CERT (IP ADDRESS) FOR ECC KEYS

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	SHA384WithRSAEncryption {1 2 840 113549 1 1 12}
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
Subject Public Key Information	256 bit prime, 233 bit binary, id-ecPublicKey {1 2 840 10045 2 1} or greater as specified in Section 6.1.5.
Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no Octet String **Note:** CA software adds the Subject Key Identifier from the CA that issued this certificate
Subject Key Identifier	c=no Octet String) **Note:** CA software calculates a SHA-1 hash of the Subject Public Key for this certificate
Key Usage	c=yes; digitalSignature
Extended Key Usage	c=no; id-kp-serverAuth {1 3 6 1 5 5 7 3 1} (Optional) id-kp-clientAuth {1 3 6 1 5 5 7 3 2}
Certificate Policies	c=no; {1.3.27.16.1.1.0.8} MediumDeviceHardware {2 23 140 1 2 2} Organization Validated {1 3 27 16 1 1 0} ICAO Certificate Policy {1 3 6 1 4 1 44109 0 1} FAA NPE Certificate Policy CPS URI:<FAA NPE CP file via a publicly available URL> Shall select one of the following OIDs based protection of private key or key usage for the end entity certificate: {1.3.27.16.1.1.0.2} LowDevice {1.3.27.16.1.1.0.3} Low-TSPMediatedSignature {1.3.27.16.1.1.0.5} MediumDevice {1.3.27.16.1.1.0.6} Medium-TSPMediatedSignature {1.3.27.16.1.1.0.8} MediumDeviceHardware

4171

Subject Alternative Name	c=no (Mandatory) IP Address Shall include one or more iPAddress=additional name where “additional name” is per section 7.1.4
Authority Information Access	c=no FAA IDMS Issuing CA certificate via a publicly available URL OCSP Responder service for FAA IDMS Issuing CA via a publicly available URL
CRL Distribution Points	c = no Latest CRL file published by FAA IDMS Issuing CA via a publicly available URL
Embedded SCTs	c=no (WebTrust Mandatory) This extension must appear in all TLS Server certificates issued by an Issuing CA participating in Web Browser Root Programs.

4172

4173

10.8 TLS CLIENT AUTH CERT FOR RSA KEYS

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	SHA384WithRSAEncryption {1 2 840 113549 1 1 12}
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
Subject Public Key Information	2048-bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no Octet String **Note:** CA software adds the Subject Key Identifier from the CA that issued this certificate
Subject Key Identifier	c=no Octet String **Note:** CA software calculates a SHA-1 hash of the Subject Public Key for this certificate
Key Usage	c=yes digitalSignature
Extended Key Usage	c=no id-kp-clientAuth {1.3.6.1.5.5.7.3.2}
Certificate Policies	c=no {2 23 140 1 2 2} Organization Validated {1 3 27 16 1 1 0} ICAO Certificate Policy {1 3 6 1 4 1 44109 0 1} FAA NPE Certificate Policy CPS URI:<FAA NPE CP file via a publicly available URL> Shall select one of the following OIDs based protection of private key or key usage for the end entity certificate: {1.3.27.16.1.1.0.2} LowDevice {1.3.27.16.1.1.0.3} Low-TSPMediatedSignature {1.3.27.16.1.1.0.5} MediumDevice {1.3.27.16.1.1.0.6} Medium-TSPMediatedSignature {1.3.27.16.1.1.0.8} MediumDeviceHardware

Subject Alternative Name	c=no; (Mandatory) Host URL | IP Address | Host Name Shall include a dNSName=additional name or iPAddress=additional name where “additional name” is per section 7.1.4
Authority Information Access	c=no FAA IDMS Issuing CA certificate via a publicly available URL OCSP Responder service for FAA IDMS Issuing CA via a publicly available URL
CRL Distribution Points	c = no . Latest CRL file issued by FAA IDMS Issuing CA via a publicly available URL

4176

4177

10.9 TLS CLIENT AUTH CERT FOR ECC KEYS

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	SHA384WithRSAEncryption {1 2 840 113549 1 1 12}
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
Subject Public Key Information	256 bit prime, 233 bit binary, id-ecPublicKey {1 2 840 10045 2 1} or greater as specified in Section 6.1.5.
Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no Octet String **Note:** CA software adds the Subject Key Identifier from the CA that issued this certificate
Subject Key Identifier	c=no **Note:** CA software calculates a SHA-1 hash of the Subject Public Key for this certificate
Key Usage	c=yes digitalSignature
Extended Key Usage	c=no id-kp-clientAuth {1.3.6.1.5.5.7.3.2}
Certificate Policies	c=no {2 23 140 1 2 2} Organization Validated {1 3 27 16 1 1 0} ICAO Certificate Policy {1 3 6 1 4 1 44109 0 1} FAA NPE Certificate Policy CPS URI:<FAA NPE CP file via a publicly available URL > Shall select one of the following OIDs based protection of private key or key usage for the end entity certificate: {1.3.27.16.1.1.0.2} LowDevice {1.3.27.16.1.1.0.3} Low-TSPMediatedSignature {1.3.27.16.1.1.0.5} MediumDevice {1.3.27.16.1.1.0.6} Medium-TSPMediatedSignature {1.3.27.16.1.1.0.8} MediumDeviceHardware

Subject Alternative Name	c=no; (Mandatory) Host URL | IP Address | Host Name Shall include a dNSName=additional name or ipAddress=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 may contain id-ad-ocsp access method entry with HTTP URL for the Issuing CA OCSP Responder FAA IDMS Issuing CA certificate via a publicly available URL OCSP Responder service for FAA IDMS Issuing CA via a publicly available URL
CRL Distribution Points	c = no Latest CRL file issued by FAA IDMS Issuing CA via a publicly-available URL

4180

4181

4182

10.10 NPE DIGITAL SIGNATURE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	SHA384WithRSAEncryption {1 2 840 113549 1 1 12}
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
Subject Public Key Information	RSA: 2048-bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1} ECC: 256 bit prime, 233 bit binary, id-ecPublicKey {1 2 840 10045 2 1} or greater as specified in Section 6.1.5.
Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no Octet String **Note:** CA software adds the Subject Key Identifier from the CA that issued this certificate
Subject Key Identifier	c=no **Note:** CA software calculates a SHA-1 hash of the Subject Public Key for this certificate
Key Usage	c=yes; digitalSignature nonRepudiation
Extended Key Usage	c=no id-messageSigning {1 3 6 1 4 1 11243 20 1 1}
Certificate Policies	c=no{1 3 27 16 1 1 0} ICAO Certificate Policy {1 3 6 1 4 1 44109 0 1} FAA NPE Certificate Policy CPS URI:<FAA NPE CP file via a publicly available URL> Shall select one of the following OIDs based protection of private key or key usage for the end entity certificate: {1.3.27.16.1.1.0.2} LowDevice {1.3.27.16.1.1.0.3} Low-TSPMediatedSignature {1.3.27.16.1.1.0.5} MediumDevice {1.3.27.16.1.1.0.6} Medium-TSPMediatedSignature {1.3.27.16.1.1.0.8} MediumDeviceHardware

Authority Information Access	c=no FAA IDMS Issuing CA certificate via a publicly available URL OCSP Responder service for FAA IDMS Issuing CA via a publicly available URL
CRL Distribution Points	c = no . Latest CRL file issued by FAA IDMS Issuing CA via a publicly available URL

4185

4186

4187

4188

4189

4190

10.11 OCSP RESPONDER CERTIFICATE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	SHA384 WithRSAEncryption {1 2 840 113549 1 1 12}
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
Subject Public Key Information	2048-bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no Octet String **Note:** CA software adds the Subject Key Identifier from the CA that issued this certificate
Subject Key Identifier	c=no **Note:** CA software calculates a SHA-1 hash of the Subject Public Key for this certificate
Key Usage	c=yes (Mandatory) digitalSignature
Extended Key Usage	c=yes id-kp-OCSPSigning
Certificate Policies	c=no; {1 3 27 16 1 1 0} ICAO Certificate Policy {1 3 6 1 4 1 44109 0 1} FAA NPE Certificate Policy CPS URI:<FAA NPE CP file via a publicly available URL> Shall select one of the following OIDs based protection of private key or key usage for the end entity certificate: {1.3.27.16.1.1.0.2} LowDevice {1.3.27.16.1.1.0.3} Low-TSPMediatedSignature {1.3.27.16.1.1.0.5} MediumDevice {1.3.27.16.1.1.0.6} Medium-TSPMediatedSignature {1.3.27.16.1.1.0.8} MediumDeviceHardware
id-pkix-ocsp-nocheck {1 3 6 1 5 5 7 48 1 5}	c=no Null

10.12 SCVP SERVER CERTIFICATE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	SHA384 WithRSAEncryption {1 2 840 113549 1 1 12}
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	RSA: 2048-bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1} ECC: ecdsa-with-SHA384 {1.2.840.10045.4.3.2}
Signature Algorithm	SHA256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no Octet String **Note:** CA software adds the Subject Key Identifier from the CA that issued this certificate
Subject Key Identifier	c=no Octet String **Note:** CA software calculates a SHA-1 hash of the Subject Public Key for this certificate
Key Usage	c=yes contentCommitment digitalSignature
Extended Key Usage	C=yes id-kp-scvpServer
Certificate Policies	c=no {1 3 27 16 1 1 0} ICAO Certificate Policy {1 3 6 1 4 1 44109 0 1} FAA NPE Certificate Policy CPS URI:<FAA NPE CP file via a publicly available URL> Shall select one of the following OIDs based protection of private key or key usage for the end entity certificate: {1.3.27.16.1.1.0.2} LowDevice {1.3.27.16.1.1.0.3} Low-TSPMediatedSignature {1.3.27.16.1.1.0.5} MediumDevice {1.3.27.16.1.1.0.6} Medium-TSPMediatedSignature {1.3.27.16.1.1.0.8} MediumDeviceHardware
Subject Alternate Name	c=no HTTP URL for the SCVP Responder

Field	Value
Authority Information Access	c=no FAA IDMS Issuing CA certificate via a publicly available URL OCSP Responder service for FAA IDMS Issuing CA via a publicly available URL
CRL Distribution Points	c = no Latest CRL file issued by FAA IDMS Issuing CA via a publicly available URL

4194

4195

4196

4197

4198

4199

4200

10.13 INTERNAL ROOT CA

Base Certificate	Value		
Cert Type	CA		
Cert Profile Name	INTERNAL ROOT CA		
Version	V3 (2)		
Serial Number	Generate a non-sequential number containing 64 bits based on a cryptographically secure pseudorandom number generator (CSPNG)		
Issuer Signature Algorithm	SHA512WithRSAEncryption {1 2 840 113549 1 1 13}		
Issuer Distinguished Name	**Attribute**	**Attribute Value**	**Encoding**
	C	US	PrintableString
	O	Federal Aviation Administration	UTF8String
	CN	Common Name conforming to section 7.1.4.1 of the NPE Certificate Policy	UTF8String
Validity Period Not Before	ZZZZ/MM/DD HH:MM:SS Z **Note:** CA software uses the certificate generation date and time expressed in UTC Time during the key ceremony		
Validity Period Not After	ZZZZ/MM/DD HH:MM:SS Z **Note:** CA software uses the certificate generation date and time plus **20 years (7,306 days)** expressed in UTC Time		
Subject Distinguished Name	**Attribute**	**Attribute Value**	**Encoding**
	C	US	PrintableString
	O	Federal Aviation Administration	UTF8String
	CN	Must be the same as the Issuer Distinguished Name	UTF8String
Subject Public Key Info	4096-bit		
Signature Algorithm	SHA512WithRSAEncryption {1 2 840 113549 1 1 13}		
Certificate Extensions	Value		
Extension	**Criticality**	**Description**	**Setting**

Subject Key Identifier	False	Octet String **Note:** CA Software calculates a SHA-1 hash of the Subject Public Key for this certificate	
Key Usage	True	Key Certificate Signature	Enable
		CRL Signature	Enable
Extended Key Usage	False	Key Cert Sign	Enable
		CRL Sign	Enable
Basic Constraints	True	CA	Enable
		Path Length Constraints	Absent

4202

4203

4204

10.14 INTERNAL TLS CERTIFICATE

Base Certificate	Value		
Cert Type	CA		
Cert Profile Name	INTERNAL TLS CERTIFICATE		
Version	V3 (2)		
Serial Number	Unique identifier Note: CA software generates a non-sequential number containing 64 bits based on a cryptographically secure pseudorandom number generator (CSPNG)		
Issuer Signature Algorithm	SHA256WithRSAEncryption {1 2 840 113549 1 1 11}		
Issuer Distinguished Name	**Attribute**	**Attribute Value**	**Dictionary String 1**
	C	US	PrintableString
	O	Federal Aviation Administration	UTF8String
	CN	FAA Internal Issuing CA	UTF8String
Validity Period Not Before	ZZZZ/MM/DD HH:MM:SS Z **Note:** CA software uses the certificate generation date and time expressed in UTCTime during the key ceremony		
Validity Period Not After	ZZZZ/MM/DD HH:MM:SS Z **Note:** CA software uses the certificate generation date and time plus **1 yeas (365 days)** expressed in UTC Time		
Subject Distinguished Name	**Attribute**	**Attribute Value**	**Dictionary String 2**
	C	US	PrintableString
	O	Federal Aviation Administration	UTF8String
	CN	Host FQDN | IP Address	UTF8String
Subject Public Key Info	2048-bit		
Signature	SHA256WithRSAEncryption {1 2 840 113549 1 1 11}		
Certificate Extensions	Value		
Extension	**Criticality**	**Description**	**Setting**
Authority Key Identifier	False	Octet String **Note:** CA software adds the Subject Public Key from the CA that issued this certificate	
Subject Key Identifier	False	Octet String **Note:** CA software calculates a SHA-1 hash of the Subject Public Key for this certificate	

Key Usage	True	Digital Signature	Enable
		Key Encipherment	Enable
Extended Key Usage	False	Server Authentication	Enable
		Client Authentication	Enable
Basic Constraints	True	CA	Enable
		Path Length Constraints	Absent
CRL Distribution Point	False	Distribution Point	Latest CRL file issued by FAA Internal Issuing CA via an internal URL FAA Internal DNS
Authority Access Information	False	CA Issuer id-kp-caIssuer	FAA Internal Issuing CA certificate via an internal URL FAA Internal DNS

4206

4207

10.15 FULL CRL PROFILE

Field	Value
Version	V2 (1)
Issuer Signature Algorithm	**Root CA:** SHA512 WithRSAEncryption {1 2 840 113549 1 1 13} **Issuing CA:** SHA384 WithRSAEncryption {1 2 840 113549 1 1 12}
Issuer Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4.1 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
CRL Extension	**Value**
CRL Number	c=no; **Note:** CA software monotonically increases integer
Authority Key Identifier	c=no Octet String **Note:** CA software adds the Subject Key Identifier for the CA issuing this CRL
CRL Entry Extension	**Value**
Reason Code	c=no; Mandatory

10.16 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
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
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

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
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
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
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

4213

4214

4215

4216

4217

10.18 CODE-SIGNING CERTIFICATE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	SHA384 WithRSAEncryption {1 2 840 113549 1 1 12}
Issuer Distinguished Name	Unique X.500 CA DN conforming to Section 7.1.4 of this CP, must be identical to the Subject Distinguished Name of the issuing CA.
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	RSA: 2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1} ECC: 256 bit prime, 233 bit binary, id-ecPublicKey {1 2 840 10045 2 1} or greater as specified in Section 6.1.5.
Signature Algorithm	RSA: SHA256 WithRSAEncryption {1 2 840 113549 1 1 11} ECC: ecdsa-with-SHA384 {1 2 840 10045 4 3 3}
Extension	**Value**
Authority Key Identifier	c=no Octet String **Note:** CA software adds the Subject Key Identifier for the CA that issued this certificate
Subject Key Identifier	c=no Octet String **Note:** CA software calculates a SHA1 hash of the Subject Public Key for this certificate
Key Usage	c=yes; digitalSignature
Extended Key Usage	c=no codeSigning
Certificate Policies	c=no {1 3 27 16 1 1 0} ICAO Certificate Policy {1 3 6 1 4 1 44109 0 1} FAA NPE Certificate Policy CPS URI:<FAA NPE CP file via a publicly available URL> Shall select one of the following OIDs based protection of private key or key usage for the end entity certificate: {1.3.27.16.1.1.0.2} LowDevice {1.3.27.16.1.1.0.3} Low-TSPMediatedSignature {1.3.27.16.1.1.0.5} MediumDevice {1.3.27.16.1.1.0.6} Medium-TSPMediatedSignature {1.3.27.16.1.1.0.8} MediumDeviceHardware
Subject Alternative Name	c=no; Mandatory DN of the Subscriber
Authority Information Access	c=no

Field	Value
	FAA Internal Issuing CA certificate via an internal URL OCSP Responder service for FAA IDMS Internal Issuing CA via an internal URL
CRL Distribution Points	c = no. Latest CRL file issued by FAA IDMS Internal CA via an internal URL

4219

4220

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/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.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
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
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
IAO	Information Assurance Officer
OA	FAA Operational Authority
FAA-WG	FAA Working Group
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

4224

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).
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 message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the Private Key that corresponds to the Public Key in the signer's digital Certificate; and (2) whether the message has been altered since the transformation was made. Fills the role of a Subscriber for NPEs that are named as Public Key Certificate Subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this CP.
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.
Duration	A field within a Certificate, which is composed of two subfields; "date of issue" and "date of next issue".

Encryption Certificate	A Certificate containing a Public Key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.
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 Administrator (OAA)	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 Policy Management Authority for: • Interpreting the Certificate Policies that were selected or defined by the Policy Management Authority. • 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, or a digital Non-Person Entity under the control of another person.
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)	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. For the CA, the PMA is the PMA. As specified in the applicable Charter, the Policy Management Authority may be responsible for managing some dispute resolution amongst the TF 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' law and Entity 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/Trusted Agent is not in the same physical location as the Applicant/Subscriber. The RA/Trusted Agent controls a device, which is utilized by the Applicant/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 control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements. [NS4009]
Update (a Certificate)	The act or process by which data items bound in an existing Public Key Certificate, especially authorizations granted to the subject, are changed by issuing a new Certificate.

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. X.509 - An ITU-T standard for a Public Key Infrastructure.
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)
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]

4227