UNITED STATES

DEPARTMENT OF STATE

DEPARTMENT OF STATE (DOS)
PUBLIC KEY INFRASTRUCTURE (PKI)

X.509 CERTIFICATE POLICY

VERSION 2.1.1

November 2023

PKI POLICY MANAGEMENT AUTHORITY APPROVAL

The PKI Policy Management Authority is responsible for the development, review, and acceptance of this Certificate Policy.

This Certificate Policy has been reviewed and is approved for use.

Steven E Gregory

Digitally signed by Steven E Gregory
Date: 2023.11.02 13:04:23 -04'00'

Steven E. Gregory
DOS PKI Policy Management Authority
Division Chief IRM/FO/ITI/SI

Date

UNCLASSIFIED

DOCUMENT VERSION CONTROL

Version	Date	Author(s)	Reason For Change
1.0	December 2007	C. R. Froehlich	Publication
1.1	March 2008	R. L. Doty & C. R. Froehlich	Minor editing & FBCA cross mapping revisions
1.2	April 2008	C. R. Froehlich	FBCA cross mapping revisions
1.3	July 2008	R. L. Doty	
1.4	February 2009	C. R. Froehlich	Reflect those changes to the FBCA CP that affect the DOS CP
1.4.1	January 2011	C. R. Froehlich	Reflect those changes to the FBCA CP that affect the DOS CP
1.4.2	May 2011	C. R. Froehlich	Reflect those changes to the FBCA CP that affect the DOS CP
1.4.3	July 2011	C. R. Froehlich	Termination of FADS, cross certification with the FCPCA; Reflect those changes to the FBCA CP that affect the DOS CP
1.4.4-1.4.7	August 2011	C. R. Froehlich	Reflect those changes to the FBCA CP that affect the DOS CP
1.4.8	October 2011	C. R. Froehlich	Reflect those changes to the FBCA CP that affect the DOS CP
1.4.9	December 2011	C. R. Froehlich	Reflect those changes to the FBCA and FCPCA CPs that affect the DOS CP
1.5	December 2011	R. L. Doty	Restructuring of appendices
1.6	February 2012	C. R. Froehlich	Reflect those changes to the FBCA and FCPCA CPs that affect the DOS CP
1.7	March 2012	C. R. Froehlich	Reflect those changes to the FBCA and FCPCA CPs that affect the DOS CP

Version	Date	Author(s)	Reason For Change
1.7.1	June 2012	C. R. Froehlich & S.R. Turner	Technical edit with mapping
1.7.2	April 2013	C. R. Froehlich	Reflecting changes to the FBCA/FCPCA CPs affecting DOS CP and corrections identified in audit
1.7.3	December 2013	C. R. Froehlich	Reflecting change to FBCA/FCPCA CPs affecting DOS CP and corrections identified in audit
1.7.4	September 2016	L. Shomo	Reflecting changes to FBCA/FCPCA CPs affecting DOS CP and corrections identified in audit
1.7.5	September 2017	L. Shomo	Reflecting changes to FBCA/FCPCA CPs affecting DOS CP, addition of PIV CA2, and corrections identified in audit
1.7.6	May 2018	L. Shomo & R. L. Doty	Removal of references to Common Policies, clarification of Sections 5.8 and 6.3.2, and reflect changes to the FBCA CP that affect the DOS CP. Clean up document formatting.
1.7.7	September 2018	L. Shomo	Add DOS Wildcard Certificate policy, change PKI Sponsor security clearance requirements, clarification of PMA and PM Roles description, and reflect changes to the FBCA CP.
1.7.8	March 2021	L. Shomo	Reflect changes to the FBCA CP, address audit and annual review findings, revise process for updating the CP, update information including removing references to the PIV CA.

Version	Date	Author(s)	Reason For Change
1.7.9	July 2021	L. Shomo	Address FPKI annual review comments.
2.0	May 2023	L. Shomo	Reflect update of the FBCA CP to Version 3 and 3.1, including incorporating key recovery policy and updates to audit and archive. Add an administrator authentication certificate policy, and certificate suspension. Modify Group and Role certificate requirements. Address compliance audit and annual review findings. Update Appendices.
2.0.1	August 2023	L. Shomo	Minor grammar, punctuation, spelling and format corrections.
2.1	September 2023	L. Shomo	Reflect update of the FBCA CP to Version 3.2 and address FPKI 2022 Annual Review mapping variance findings.
2.1.1	November 2023	L. Shomo	Address two KRA control of KED Key and third-party key recovery in Section 5.2.2.

TABLE OF CONTENTS

TABLE OF TABLES

1. INTRODUCTION

The United States Department of State (DOS[1]) has implemented a Public-Key Infrastructure (PKI) that provides a method for securing transmission of information across department information system assets, supporting the verification of an entity's identity for physical and logical access control, and implementing legally binding digital signatures, in a Sensitive But Unclassified (SBU) environment.

A PKI consists of products and services that provide and manage X.509 certificates for public key cryptography. Public key cryptography is an information technology security service that can provide identity authentication, data integrity verification, technical non-repudiation, confidentiality (i.e., privacy), and digital signatures for electronic transactions.

This Certificate Policy (CP) defines multiple certificate policies for use by the Department of State PKI X.509 Certification Authorities (CAs) to facilitate interoperability between the DOS PKI domain, the PKI domains cross-certified with the Federal Bridge Certification Authority (FBCA), the Federal Common Policy Framework (FCPF) PKI domain, and other Entity PKI domains. The policies represent five different assurance levels (Rudimentary, Basic, Medium, Medium Hardware, and High) for public key certificates. The level of assurance refers to the strength of the binding between the public key and the entity whose subject name is cited in the certificate, the mechanisms used to control the use of the private key, and the security provided by the PKI itself.

All subordinate CA certificates contain a NIST-registered Certificate Policy Object Identifier (OID), which a Relying Party may use to decide whether a certificate is trusted for a particular purpose. The OID corresponds to a specific level of assurance established by this CP. Each end-entity or subordinate CA certificate issued by the Department will assert the appropriate levels of assurance in the *certificatePolicies* extension. Any use of or reference to this CP outside the purview of the Department of State PKI Policy Management Authority (DOS PKI PMA) is completely at the using party's risk. An Entity outside the Department of State must not assert the DOS PKI CP OIDs in any certificates the Entity CA issues, except in the *policyMappings* extension establishing an equivalency between a DOS PKI CP Policy and a Policy in that Entity CA's CP.

This CP is consistent with the *Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (PKIX) RFC 3647, Certificate Policy and Certification Practices Framework*. Users must interpret the terms and provisions of this CP under, and be governed by, applicable Federal law. This policy is also in consonance with and augments the information system security requirements in Foreign Affairs Manual, Chapter 12 Section 600 (12 FAM 600).

The reliability of the public key cryptography portion of a security solution is a direct result of the secure and trustworthy operation of an established PKI, including equipment, facilities, personnel, and procedures. This CP applies to certificates issued to person entities (PE)s

[1] The "DOS" acronym used in this document refers to the Department of State as an entity, and should not be confused with the term "DOS PKI," which is a naming convention used by the Department to include all non-specialty PKIs operating within the Department. This document applies *only* to the DOS PKI.

including Federal employees, contractors, and other affiliated personnel for the purposes of authentication, digital signature, and confidentiality. This CP also applies to certificates issued to non-person entities including devices, systems, and applications for the purposes of authentication, and confidentiality. The Subscriber policies require Federal employees, contractors, and other affiliated personnel to use Federal Information Processing Standards Publication (FIPS Pub) 140 validated cryptographic modules for cryptographic operations and the protection of trusted private keys. The Subscriber polices for devices also require the use of FIPS Pub 140 validated cryptographic modules for cryptographic operations and the protection of trusted private keys.

1.1 OVERVIEW

1.1.1 Certificate Policy

The United States *Department of State Public Key Infrastructure X.509 Certificate Policy* (DOS PKI CP) is the policy under which a designated Department component establishes and operates a Root Certification Authority (Root CA) and its subordinate Certification Authorities[2]. The CP defines policies that establish distinct assurance levels for certificates issued by the DOS PKI CAs. Relying parties may base the reliance they choose to place on a given level of certificate assurance on the following:

- Amount and type of inherent risk of an activity
- Consequence of failure
- Use of risk mitigation controls

This document does not define certificate policy for CAs operated by external entities that communicate with the Department, and who issue their own certificates.

In addition, this document defines the creation and management of X.509, version 3, public key certificates for use in applications requiring trusted communication between networked computer-based systems. Such applications include but are not limited to the following examples: electronic mail; transmission of SBU[3] information; signature of electronic forms; signature of contracts; and authentication of infrastructure components such as web servers, firewalls, directories, and mobile code.

Specific subordinate CAs in the DOS PKI also issue certificates for Personal Identity Verification (PIV) credentials issued to Department employees, contractors, and other affiliated personnel and derived-PIV credentials issued to mobile devices. These PIV credential-related

[2] Within this policy, the generic term "DOS PKI" refers to any and all non-specialty PKI infrastructures operated by the Department to support its Sensitive But Unclassified (SBU) environment. Unless otherwise specified, the term "AD CA" generally refers to all PKI Certificate Authorities operating under the Active Directory architecture.

[3] The existence and use of the DOS PKI does not authorize or permit the transmission of classified information over unclassified networks. A separate PKI Infrastructure is established under CNSS Instruction No. 1300 for that purpose.

activities are governed by the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework* (FCPF CP), not by this DOS PKI CP.[4]

The DOS PKI does not issue PIV-I Cards; however it issues DOS Facility Logical Access Cards (FLAC) whose card authentication certificate asserts the id-fpki-common-pivi-cardAuth certificate policy.

1.1.2 Relationship between the DOS PKI CP and the DOS PKI CPS

The DOS PKI CP states what assurance Subscribers can place in a certificate issued by the DOS PKI CAs. The DOS PKI Certification Practices Statement (CPS) addresses how the Active Directory Root CA (AD Root CA), the subordinate Active Directory High Assurance CA (AD HACA), and for non-PIV-related certificates how the subordinate PIV CA2, establish that assurance.

For PIV-related certificates issued by the subordinate PIV CA2 and DPC CA, the FCPF CP states what assurance Subscribers can place in those certificates, and the DOS PKI CPS addresses how the PIV CA2 and DPC CA establish that assurance.

1.1.3 Relationship between the DOS PKI CP, FBCA CP, FCPF CP, and Other Entity CPs

The Federal PKI Policy Authority (FPKIPA) maps certificate policies and their levels of assurance between the DOS PKI CP and the *X.509 Certificate Policy for the Federal Bridge Certification Authority* (FBCA CP) and *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework* (FCPF CP). The relationship between these CPs is asserted via the *policyMappings* extension in a cross-certificate issued by the Federal Common Policy Root CA (FCPCA) to the DOS PKI AD Root CA citing the equivalent FCPF CP and FBCA CP certificate policy for each applicable DOS PKI certificate policies.

The FPKIPA also maps levels of assurance between the FBCA CP and various other Entity PKI's CPs to facilitate trust and interoperability among a community of cross-certified PKIs. The DOS PKI PMA will generally accept the assurance level mapping determinations of the FPKIPA.

In the same manner that the FPKIPA maps levels of assurance between the FBCA CP and the DOS PKI CP, the DOS PKI PMA may map levels of assurance between another Entity CP to those in the DOS PKI CP, in order to establish a trust and interoperability relationship. The DOS PKI PMA makes the final determination that an external PKI's certificate policies offer appropriately equivalent levels of assurance to the certificate policies specified in the DOS PKI CP, based on the analysis and recommendations of the DOS PKI Management Authority (DOS PKI MA). The DOS PKI MA may respond to such decisions by implementing trust of the External Entity's certificates by methods including but not limited to the following:

[4] The PIV CA2 issues PIV credential certificates governed by the FCPF CP, and also issues certificates that are not related to PIV credentials which are governed by the DOS PKI CP.

- Issuing a cross-certificate to the external PKI CA that maps their policies to DOS PKI policies
- Adding the external PKI CA to a DOS PKI trust list
- Placing the external PKI CA's certificate in appropriate certificate trust stores

The DOS PKI PMA or DOS PKI MA must notify the FPKIPA of any cross certificates it issues to external PKIs.

1.1.4 Scope

This CP applies to certificates issued to CAs, devices, applications, Federal employees, contractors, and other affiliated personnel. This CP also applies to certificates issued to organizations and/or groups of people and to roles, with the understanding that such certificates, by the nature of such use, lose the capacity for technical non-repudiation.

Programs that carry out or support the mission of the Department of State require services such as authentication, confidentiality, data-integrity, technical non-repudiation, and logical access control. An array of network security components, such as workstations, guards, firewalls, routers, in-line network encryptors, and trusted database servers, satisfy these service requirements. The use of public key cryptography supports and complements the operation of these components. This CP addresses a level of assurance comparable to the FBCA High and FCPF CP High Assurance Policies, and all lower assurance levels. Services provided by the DOS PKI include:

- Key generation, storage, and recovery
- Certificate generation,renewal, re-key, key recovery, modification, revocation, and distribution
- Certificate Revocation List (CRL) generation and distribution
- Online certificate status services
- Directory management of certificate related items
- Certificate token initialization, programming, and management
- System management functions (e.g., security audit, configuration management, archive)

The CP also defines requirements to ensure the security of these services:

- Subscriber identification and authorization verification
- Control of computer and cryptographic systems
- Operation of computer and cryptographic systems
- Usage of keys and public key certificates by Subscribers
- Rules defining limitations of liability and to provide a high degree of certainty

1.1.5 Interaction with PKIs External to the Federal Government

The DOS PKI AD Root CA achieves interoperation with non-Federal CAs that issue under different policies by policy mapping and cross certification through the FBCA, the FCPCA, or directly with the agency in question. The DOS PKI AD Root CA extends interoperability with non-Federal entities only when it is beneficial to the Federal Government and to the mission of the Department. The DOS PKI PMA or DOS PKI MA will notify the FPKIPA of any cross certificates it issues to external PKIs.

When the DOS PKI needs to directly establish interoperability with an External Entity, the DOS PKI MA must develop a Memorandum of Agreement (MOA) to be signed by the DOS Principal Deputy Chief Information Officer (PDCIO) and an authorized representative of the other entity. The MOA must detail the agreement between the Entity and the DOS PKI covering interoperability between the two entities which is enabled via cross-certification between them. Specifically, it sets forth the rights, responsibilities and reservations of both Parties governing the Entity's interoperation with the DOS PKI.

1.2 DOCUMENT NAME AND IDENTIFICATION

The official title of this CP is the *U.S. Department of State Public Key Infrastructure X.509 Certificate Policy*. There are eight certificate policies specified at five levels of assurance in this Certificate Policy. Subsequent sections of this document define the levels of assurance asserted by this policy.

Each certificate policy has a certificate policy Security Object Identifier (OID) for the specific policy, that is asserted in the *certificatePolicies* extension in certificates issued by DOS CAs within the DOS PKI.

The National Institute of Standards and Technology (NIST) assigned the following IETF notation arc for DOS CPs: 2.16.840.1.101.3.2.1.6.

International Organization for Standardization (ISO) notation represents this as:

> state-policies OBJECT IDENTIFIER: = {joint-iso-ccitt (2) country (16) us (840) organization (1) gov (101) csor (3) pki (2) cert-policy (1) state-policies (6)}

The Department has registered the following certificate policies (in order of increasing assurance) in the NIST Computer Security Objects Registry (CSOR) under this arc:

Table 1-1 DOS Certificate Policy OIDs

Certificate Policy	Certificate Policy OID
id-state-certpcy-rudimentaryAssurance[5]	::= {2.16.840.1.101.3.2.1.6.1}

[5] DOS previously referred to the Rudimentary Assurance level by the common name “Basic Assurance” for internal Department clarity.

Table 1-1 DOS Certificate Policy OIDs

Certificate Policy	Certificate Policy OID
id-state-certpcy-basicAssurance[6]	::= {2.16.840.1.101.3.2.1.6.2}
id-state-certpcy-mediumAssurance[7]	::= {2.16.840.1.101.3.2.1.6.3}
id-state-certpcy-mediumHardware	::= {2.16.840.1.101.3.2.1.6.12}
id-state-certpcy-highAssurance	::= {2.16.840.1.101.3.2.1.6.4}
id-state-certpcy-administratorAuth	::= {2.16.840.1.101.3.2.1.6.13}
id-state-certpcy-mediumDevice	::= {2.16.840.1.101.3.2.1.6.37}
id-state-certpcy-mediumDeviceHardware	::= {2.16.840.1.101.3.2.1.6.38}

The levels of assurance of each of the certificate policies is shown in the following table.

Table 1-2 Assurance Level of Certificate Policies

Certificate Policy	Assurance Level
id-state-certpcy-rudimentaryAssurance	Rudimentary
id-state-certpcy-basicAssurance	Basic
id-state-certpcy-mediumAssurance	Medium
id-state-certpcy-mediumHardware	Medium Hardware
id-state-certpcy-highAssurance	High
id-state-certpcy-administratorAuth	High
id-state-certpcy-mediumDevice	Medium
id-state-certpcy-mediumDeviceHardware	Medium Hardware

[6] DOS previously referred to the Basic Assurance level by the common name “Low Assurance” for internal Department clarity.

[7] DOS previously referred to all Medium Assurance level certificates by the common name “Moderate Assurance” for internal Department clarity.

Certificates valid for the following policies are issued to Human Subscribers:

Table 1-3 Human Subscriber Certificates

Certificate Type	Certificate Policy
Administrator Authentication certificate	id-state-certpcy-administratorAuth
FLAC Authentication certificate	id-state-certpcy-mediumHardware
FLAC Digital Signature certificate	id-state-certpcy-mediumHardware
FLAC Key Management Key certificate	id-state-certpcy-mediumHardware
SNAP Digital Signature certificate	id-state-certpcy-highAssurance
SNAP Key Management Key certificate	id-state-certpcy-highAssurance
Yubikey Digital Signature certificate	id-state-certpcy-mediumHardware id-state-certpcy-highAssurance
Yubikey Key Management Key certificate	id-state-certpcy-mediumHardware id-state-certpcy-highAssurance
Role-Based Digital Signature certificate	id-state-certpcy-mediumHardware
Role-based Key Management Key certificate	id-state-certpcy-mediumHardware
Group Digital Signature certificate	id-state-certpcy-mediumHardware
Group Key Management Key certificate	id-state-certpcy-mediumHardware
Code Signing certificate	id-state-certpcy-highAssurance
All other hardware-based certificates	id-state-certpcy-mediumHardware id-state-certpcy-highAssurance
All software-based certificates	id-state-certpcy-rudimentaryAssurance id-state-certpcy-basicAssurance id-state-certpcy-mediumAssurance

The DOS PKI AD Root CA is not subordinate to the FCPCA, but policies in the DOS PKI CP have been cross-mapped at the Medium Assurance level and above to non-PIV-specific policies in the FCPF CP.

The DOS PKI CP rudimentaryAssurance and basicAssurance policies are not cross-certified to the similar FBCA policies.

The requirements associated with the Medium Hardware policy are identical to those defined for the Medium Assurance policy except for the Subscriber cryptographic module requirements (see Section 6.2.1).

The CPS for the AD Root CA and for subordinate CAs specify which policy OIDs that CA asserts.

The DOS PKI does not assert the Medium and Medium Hardware Commercial Best Practice (Medium-CBP and MediumHW-CBP) policies addressed in the FBCA CP.

The DOS PKI does not issue certificates for Personal Identity Verification Interoperable (PIV-I) cards as defined in the FBCA CP.

For DOS Facility Logical Access Cards (FLAC) issued by the PIV CA2, the card authentication certificate asserts the id-fpki-common-pivi-cardAuth certificate policy defined by the FCPF CP.

Certificates valid for the following policies are issued to Device Subscribers:

Table 1-4 Device Subscriber Certificates

Certificate	Certificate Policy
For devices that use a FIPS 140 Level 1 cryptographic module	id-state-certpcy-mediumDevice
For devices that use a FIPS 140 Level 2 or higher cryptographic modules	id-state-certpcy-mediumDeviceHardware

In this document, the term “device” is defined as a non-person entity (e.g., a hardware device/system or software application).

The use of the *mediumDevice* and *mediumDeviceHardware* policies is restricted to, and required in certificates issued to devices, systems, and applications.

The requirements associated with the *mediumDevice* and *mediumDeviceHardware* policies are identical to those defined for the Medium Assurance and Medium Hardware Assurance policies, respectively, except for identity proofing, re-key, and activation data.

1.3 PKI PARTICIPANTS

The Under Secretary for Management has assigned responsibility for the Department of State PKI Program to the Bureau of Information Resource Management (IRM). DOS 1 FAM 275.2-3 outlines this responsibility. The following are roles relevant to the administration and operation of the DOS PKI and its CAs.

1.3.1 PKI Authorities

The Department of State Chief Information Officer (CIO) heads the IRM Bureau with the PDCIO responsible for overseeing operations through the Deputy Chief Information Officers. The IRM Bureau is responsible for funding PKI, management of the PKI investment, and validation of PKI hardware and software configurations through the Department Information Technology Configuration Control Board (IT-CCB).

The DOS Deputy Chief Information Officer has delegated the DOS PKI PMA role to the Chief of the Systems Integrity (SI) Division.

1.3.1.1 PKI Policy Management Authority

The DOS PKI Policy Management Authority (DOS PKI PMA) provides senior management authority over the Department's PKIs. As such, this individual is responsible for interfacing with all Department management, and determining such issues as policy, budgets, cross certification and subordination, and continuity of operations and relocation during an emergency.

The DOS PKI PMA ensures the conformity to central Department policy for PKI implementation and operation; and coordinates with other bureaus, offices, and posts to ensure installation of one PKI solution throughout the Department. The DOS PKI PMA approves PKI CP and CPSs, designates audit authorities, and approves Certificate Management Authority (CMA) deficiency remedial actions, based on the recommendation of the DOS PKI Management Authority (DOS PKI MA).

The PDCIO executes Memoranda of Agreement (MOA) with the FPKIPA, and any Entities seeking direct cross certification, setting forth the respective responsibilities and obligations of both parties, and the mappings between the certificate levels of assurance contained in the respective CP.

The DOS PKI PMA must make the determination that other, non-Department of State Certificate Policies offer appropriately equivalent levels of assurance to the Department of State Certificate Policies. The DOS PKI may respond to such decisions by implementing trust of the External Entity's certificates by methods including but not limited to the following:

- Issuing a cross-certificate to the external PKI CA that maps their policies to DOS PKI policies
- Adding the external PKI CA to a DOS PKI trust list
- Placing the external PKI CA's certificate in appropriate certificate trust stores

The DOS PKI PMA must make information regarding such equivalency determinations available to Department of State Subscribers and Relying Parties. The DOS PKI PMA may, at his or her discretion, officially delegate signature and approval authority for the PKI Certificate Policy and Certification Practices Statements, designation of audit authorities, and approval of deficiency remedial actions, to the DOS PKI MA. The DOS PKI PMA may also delegate the authority to execute the MOA with the FPKIPA and any Entities seeking direct cross certification, as well as the authority to make the determination that other, non-Department of State Certificate Policies offer appropriately equivalent levels of assurance to the Department of State Certificate Policies to the DOS PKI MA. The DOS PKI PMA shall be responsible for notifying the FPKIPA of any change to the DOS PKI infrastructure that has the potential to affect the FPKI operational environment at least two weeks prior to implementation; all new artifacts (CA certificate, Certificate Revocation List Distribution Point (CRL DP), Authority Information Access (AIA) and/or Subject Information Access (SIA) Uniform Resource Locators (URLs), etc.) produced as a result of the change must be provided to the FPKIPA within 24 hours following implementation.

The DOS PKI PMA must be a Department of State direct-hire employee.

1.3.1.2 PKI Management Authority

The Division Chief, Systems Integrity Division is the DOS PKI MA. The DOS PKI MA has oversight responsibilities for the DOS PKI Program. The DOS PKI MA enforces Department policies, including the DOS PKI CP and FPKI policies to the extent that they apply, and ensures representation of the DOS PKI Program and the Department's interests in all internal and external matters and bodies relative to PKI technology at both the unclassified and classified levels, directly or through the DOS PKI Operational Authority (DOS PKI OA).

The DOS PKI MA has management responsibility for the following:

- Managing the process for review, modification, and publication of the DOS PKI CP and all associated CPSs in support of the DOS PKI PMA; and approving recommendations to the DOS PKI PMA regarding such modifications and of concurrent changes to Department policies and procedures resulting from such changes
- Managing the review and mapping, by the DOS PKI OA and PKI Program Office (DOS PKIPO) staff, of applications received from external entities seeking direct cross certification and interoperability with the DOS PKI AD Root CA
- Ensuring the continued conformance of cross-certified Entities with applicable requirements using the DOS PKI OA and DOS PKIPO staff
- Providing management support to necessary programmatic, infrastructure, and operational changes to the PKI Program; and, managing administrative processes (e.g., budget, security, facilities, etc.) in support of the PKI Program
- Overseeing implementation of corrective actions or other measures as appropriate to maintain cross certification and Certification and Accreditation
- Notifying the FPKIPA, on behalf of the DOS PKI PMA, of any change to the DOS PKI infrastructure that has the potential to affect the FPKI operational environment at least

two weeks prior to implementation; all new artifacts (CA certificates, CRL DP, AIA and/or SIA URLs, etc.) produced because of the change must be provided to the FPKIPA within 24 hours following implementation.

The DOS PKI MA must be a Department of State direct-hire employee.

1.3.1.3 PKI Operational Authority

The DOS PKI MA designates the PKI Operational Authority (DOS PKI OA). The DOS PKI OA is responsible for the overall establishment, operations, control and management of the DOS PKI, including the operational requirements for the DOS PKI AD Root CA, all subordinate CAs, Certificate Status Servers (CSSs), Card Management Systems (CMSs), and Registration Authorities (RAs), excluding the CMS and RA for PIV CA2.

To satisfy specific operational requirements, the DOS PKI OA may designate DOS personnel outside the DOS PKI Program Office (DOS PKIPO) to fulfill certain RA functions including some, but not necessarily all, of the functions listed hereunder. These personnel satisfy all of the same qualifications as DOS PKIPO personnel appointed to the same function.

The DOS PKI OA has primary responsibility for:

- Supervising the development, modification, and reviews of all CPs, CPSs, and implementation guidelines
- Reviewing the results of periodic compliance audits, and implementing corrective action recommendations as appropriate
- Approving routine Change Requests (CRs)
- Validation of all key recovery requests from non-Subscriber and non-PKI Sponsor requesters inside the Department in accordance with the DOS Key Recovery Policy

The DOS PKI OA also makes recommendations for selection of the DOS PKI Program Manager (DOS PKI PM).

The DOS PKI OA must be a Department of State direct-hire employee.

1.3.1.4 PKI Program Manager

The DOS PKI PM is the individual within the DOS PKI Program Office (DOS PKIPO) who has principal responsibility for overseeing the proper operation of the DOS PKI CAs daily, including the respective CA repositories and selecting the Operational Authority staff. The DOS PKI PM approves the issuance of all wildcard certificates. The DOS PKI PM is selected by and reports to the DOS PKI OA.

The DOS PKI PM must be a Department of State direct-hire employee.

1.3.1.5 PKI Program Office

The DOS PKIPO comprises the Operational Authority staff, including both trusted (See Section 5.2.1) and non-trusted role positions. The DOS PKIPO has the following responsibilities:

- The PKI Registration Center and Deployment staff administers the Department's PKI from an operational perspective, including:
  - Controlling the registration, identification and authentication, and certificate manufacturing processes with individual offices and posts, and the Diplomatic Security Bureau, to include support to the DOS PIV Card Program
  - Publishing of certificates in the appropriate directories
  - Coordinating and performing installation worldwide of card readers and middleware
  - Reviewing name space control procedures with the Distinguished Naming Authority to ensure that distinguished names are uniquely assigned for all certificates issued under the DOS PKI CP
  - Ensuring that all aspects of CA services, operations and infrastructure related to certificates issued are performed in accordance with the requirements, representations, and warranties of the CP, the DOS Subordinate CA CPSs, and Department policy
  - Developing, coordinating, and presenting PKI Training for Systems Administrators, Local Registration Authorities, Special Agent Local Registration Authorities (SA-LRA), Information System Security Officers, and End Users; and preparing training and information materials for worldwide distribution including a security awareness and training package for PKI Sponsors on "User Rules of Behavior"
- The PKI Engineering staff manages technical operational issues, including:
  - Setting up, testing, and administering the DOS PKI CAs
  - Implementing the PKI and all hardware/software components, including approved CRs
  - Issuing and revoking certificates to subordinate CAs, and to RA Subscribers from those CAs
  - Establishing a certificate repository and certificate and authority revocation lists
  - Providing repository/directory integration support to the Department's networks
  - Administering the Department's PKI from a key management perspective, including re-key of CA signing material
  - Providing application development and modification technical support to application owners to PKI-enable applications and web sites, and developing databases to support internal and external operations
  - Integrating smart card and biometric technologies in support of logical access control
- The PKI Policy and Audit Team is responsible for:

- Creating and revising Certificate Policy and Certification Practices Statements, including evaluation of changes requested by Department of State bureaus, and recommending for approval/disapproval to the DOS PKI PMA, to maintain the level of assurance and operational practicality
- Ensuring that the DOS PKI CP and all CA CPSs continue general conformance to the FBCA/FCPF CPs and to Department of State 5 FAM and 12 FAM, respectively
- Reviewing commercial CAs that offer services to the Department by analyzing CPS documents to ensure that the practices of CAs serving the Department comply with these Certificate Policies, and recommending acceptance/rejection to the DOS PKI PMA
- Establishing and maintaining operational policy and practices for the DOS CAs and RAs
- Performing Certification and Accreditation activities, including preparation of system security plans, conducting annual system security self-assessment reviews, and preparing Plans of Action and Milestones
- Performing Backup and Contingency planning, including developing policies and procedures for system backup, key recovery and key escrow, and disaster recovery and contingency planning to ensure continuity of operations
- Participating in the Federal PKI Policy Authority and its working groups to ensure compliance to the Federal model
- Conducting liaison with other government agencies concerning PKI matters
- Acting as a focal point for DOS PKI working groups, as well as PIV working groups on PKI-related matters
- Reviewing all working group documentation prior to dissemination to the working group members and other involved parties
- Coordinating with the Department's Records Management Office to ensure compliance with Federal records management regulations, Freedom of Information and Privacy Act matters.

1.3.1.6 The Diplomatic Security Service/Domestic Operations/Domestic Facilities Protection (DS/DSS/DO/DFP)

The Diplomatic Security Service/Domestic Operations/Domestic Facilities Protection (DS/DSS/DO/DFP) staff administers the Department's One Badge Program (Personal Identity Verification (PIV) Cards, Facility Logical Access Cards (FLAC),) from an operational perspective for new and existing employee issuances, renewals, identity and/or clearance modifications, and replacement of lost, stolen, compromised or damaged cards, in accordance with *U.S. Department of State Bureau of Diplomatic Security DOS One Badge PIV Card Issuer (PCI) Operations Plan* (DS PCI OP)including:

- Validation/revalidation of identity and security clearance status of DOS government and contractor employees, and vendors

- Validation/revalidation of physical access requirements
- Confirms the conduct of requisite security briefings for cleared employees by Security Infrastructure/Information Security/Program Applications Division (DS/SI/IS/PAD)
- Preparation of the PIV and FLAC cards, including taking of digital photographs and fingerprints
- Submission, as the PIV RA, for installation of the mandatory PIV Authentication certificate on PIV cards, and installation of the FLAC Authentication certificate on FLAC cards
- Issuance of completed PIV and FLAC cards to the appropriate individuals following re-confirmation of identity
- Maintaining PIV and FLAC card registration records and documentation, including those off-line records relative to PKI
- Inventory, control and security of blank PIV and FLAC card stock issued by the DS/DO/DFP staff; the PIV Card Custodian has total control of blank card stock in accordance with the Standing Operating Procedures for Accountability and Control of Blank 64K DOS Personal ID Cards (HSPD-12 PIV and FLAC Cards).
- Receipt, security, initial revocation processing of physical access codes and PIV Authentication certificates, and destruction of surrendered, invalidated, damaged, compromised, and/or recovered PIV and FLAC cards.

1.3.2 Certification Authorities

The CA is the collection of hardware, software and operating personnel that create, sign, and issue public key certificates to Subscribers. The CA is responsible for issuing and managing certificates including:

- The certificate manufacturing process
- Publication of certificates
- Revocation of certificates
- Generation and destruction of CA signing keys
- Ensuring that all aspects of the CA services, operations, and infrastructure related to certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP.

1.3.2.1 Root Certification Authority

The AD Root CA (the collection of hardware, software, and operating personnel) is the entity established by the DOS PKI MA to certify subordinate CAs that, in turn, create, sign, and issue public key certificates to subscribers within DOS and other related PKI communities. The Department's PKI operates in a hierarchical fashion, utilizing a Root CA and subordinate CAs. The AD Root CA serves as the trust anchor for all certificates issued under this policy. The AD

Root CA also acts as the Principal CA (PCA) for DOS to receive a cross-certificate from the FCPCA.

The PCA issues either end entity certificates, or CA certificates to other Entity or external party CAs, or both. The PCA shall cross-certify with the FCPCA, and other root level CAs from other trust domains, as appropriate. The PCA must also certify CAs within DOS that are part of the subordination hierarchy (as opposed to cross certification).

The DOS must ensure that no CA under the DOS PKI shall have more than one trust path to the FCPCA.

This policy permits both off-line and online Root CA operation. The AD Root CA must be logically and/or physically isolated from the DOS network. The CMA for the DOS AD Root CA is responsible for issuing and managing certificates; and ensuring that the performance of all aspects of CA services, operations, and infrastructure related to certificates issued under this policy are in accordance with the requirements, representations, and warranties of this policy. This includes the following:

- The AD Root CA certifies subordinate CAs, which will assert one or more assurance levels defined in this CP, and outlined in the appropriate CPS
- The PCA must also comply with the requirements set forth in applicable MOA, Memorandum of Understanding (MOU), and contractual agreements with cross-certified CAs and/or other entities

1.3.2.2 Subordinate Certification Authorities

Subordinate CAs are responsible for all aspects of the issuance and management of a certificate to person entity subscribers and non-person entity subscribers (devices/systems/applications), including control over the enrollment process, the identification and authentication process, the certificate manufacturing process, publication of certificates, revocation of certificates, and re-key.

A CA which issues certificates that assert policies defined in this document and its CMA must conform to the stipulations of this document, including the following:

- Providing to the appropriate authorities a CPS, as well as any subsequent changes, for conformance assessment
- Maintaining its operations in conformance to the stipulations of the approved CPS
- Ensuring that registration information is accepted only from RAs/LRAs who understand and are obligated to comply with this policy, and operating under an approved CPS
- Including only valid and appropriate information in the certificate, and to maintaining evidence that due diligence was exercised in validating the information contained in the certificate
- Ensuring that all Subscribers (government and non-government) are informed of their obligations under Sections 1.4 and 9.6.3, including the consequences of not complying

with those obligations, and revoking the certificates of Subscribers found to have acted in a manner counter to those obligations

- Operating or obtaining the services of an online repository that satisfies the obligations under Sections 1, 9.6.1, and 9.6.5, and informing the repository service provider of those obligations if applicable

1.3.3 Card Management System

The CMS is responsible for managing the lifecycle of the cryptographic tokens containing subscriber private keys and certificates, such as smart cards or YubiKey tokens. CMAs have a responsibility to ensure that CMSs that manage the token on which their certificates reside provide a level of security commensurate with the assurance level of the certificates.

1.3.4 Registration Authority and Local Registration Authority

The DOS PKI RAs, and bureau, office, or post Local Registration Authorities (LRAs), are personnel recognized as authorized to collect and verify users' identity and information which is to be entered into the Subscriber's public key certificates. The key difference between RAs and LRAs is the nature and degree of their respective access to the DOS PKI CAs. The RA, by definition, functions as the Officer trusted role of the DOS PKI CP as defined in Section 5.2.1.1.2. The DOS PKI OA appoints RA(s) from members of the DOS PKIPO or other DOS personnel as necessary for specific operational requirements. RAs perform their functions in accordance with a CPS approved by the DOS PKI PMA.

Both Certification Authorities and Registration Authorities are termed "Certificate Management Authorities (CMA)." This policy uses the term "CMA" when a function may be assigned to either a CA or an RA, or when a requirement applies to both CAs and RAs. The term "Registration Authority" includes entities such as Local Registration Authorities (a.k.a. Trusted Agents[8]), unless otherwise specified. Section 5.2.1, Trusted Roles, lists specifically defined trusted roles, i.e., roles whose incumbents perform functions that involve the handling of sensitive cryptographic material and can thus introduce security problems to the CA if not carried out properly.

The division of Subscriber registration responsibilities between the CA and RA may vary among implementations of this CP, as outlined in the applicable CPS. All CMAs must protect Subscriber personal information from unauthorized disclosure as mandated by the Privacy Act of 1974, as amended.

The responsibility for managing and performing Registration Authority functions for the DOS PKI is divided between two DOS Bureaus. The Bureau of Diplomatic Security is responsible for managing and performing the Registration Authority functions for subscriber certificates issued from the PIV CA2 supporting the One Badge Program. The Bureau of Information Resource

[8] A "Trusted Agent" is a person who satisfies all the trustworthiness requirements for an RA, and who performs identity proofing as a proxy for the RA recording and verifying information about applicants as outlined in the applicable CPS and supporting Standard Operating Procedures.

Management is responsible for managing and performing Registration Authority functions for all other certificates issued by the DOS PKI.

1.3.5 Certificate Status Servers

The DOS PKI includes an authority that provides status information about certificates on behalf of the DOS PKI CAs through online transactions via CSSs. An example of a CSS is Online Certificate Status Protocol (OCSP) responders identified in the AIA extension. Where certificates identify the CSS as an authoritative source for revocation information, the operations of that authority are within the scope of this CP. A CSS must assert all policy OIDs for which it is authoritative. This policy does not cover OCSP servers that are locally trusted, as described in RFC 2560.

1.3.6 Key Recovery Authorities

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

- CA requirements apply to the Key Escrow Database (KED)
- RA requirements apply to Key Recovery Agent (KRA) personnel and KRA automated systems
- RA requirements apply to Key Recovery Official (KRO) personnel and KRO automated systems, when the KRO has privileged access to the KED.

1.3.6.1 Key Escrow Database

The KED is defined as the function, system, or subsystem that maintains the key escrow repository and responds to key registration requests. The KED also responds to key recovery requests from two or more KRAs or self-recovery by a current subscriber. Key escrow of Subscriber private decryption keys are authorized as described in the applicable CPS. Key escrow of Subscriber authentication and signature keys is prohibited.

Section 5.2.1.3 contains the description of Trusted Roles required to operate the KED.

1.3.6.2 Data Decryption Server

The DOS PKI has not implemented a Data Decryption Server.

1.3.6.3 Key Recovery Agent

A KRA is an individual who is authorized, as specified in the applicable Certificate Practice Statement), to recover an escrowed key. The KRAs send the recovered key to the Key Recovery Official or directly to the Requestor. The KRAs have high level, sensitive access to the KED and are considered Trusted Roles (see Section 5.2.1). KRAs can recover large numbers of keys, the number and location of KRAs should be closely controlled.

KRAs may additionally conduct requestor identity verification and authorization validation when KROs are not used.

1.3.6.4 Key Recovery Official

A Key Recovery Official (KRO) may optionally be used to support identity verification and authorization validation tasks.

1.3.7 Key Recovery Requestors

A Requestor is the person that requests the recovery of a decryption private key. A Requestor may be the Subscriber or a third-party (e.g., supervisor, corporate officer, or law enforcement officer) authorized to request recovery of a Subscriber's escrowed key on behalf of the Subscriber or on behalf of the organization. Any individual who can demonstrate a verifiable authority and a need to obtain a recovered key may be considered a Requestor.

1.3.7.1 Internal Third-Party Requestor

An Internal Third-Party Requestor is any Requestor who is in the Subscriber's supervisory chain or otherwise authorized to obtain the Subscriber's key for the Issuing Organization (i.e., the organization on behalf of which the CA issues certificates to subscribers).

1.3.7.2 External Third-Party Requestor

An External Third-Party Requestor is someone (e.g., investigator) outside the Issuing Organization with a court order or other legal instrument to obtain the decryption private key of the Subscriber.

1.3.8 Subscribers

A Subscriber is a person entity or a non-person entity (device/system/application) to whom a certificate is issued. This entity's Distinguished Name (DN) appears as the subject in the certificate, and the entity asserts that it will use the key and certificate in accordance with this policy.

Sometimes, a PKI technically considers CAs as "Subscribers." However, the term "Subscriber" as used in this document refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information.

Department of State PKI Subscribers and PKI Sponsors include but are not limited to the following categories of entities that may wish to conduct official Department business:

- Department of State personnel: Direct Hire, Locally Engaged Staff (LES), Third Country Nationals (TCNs), Part-time/Intermittent/Temporary (PIT) employees, Personal Services Contractor (PSC) employees, Direct Hire Americans overseas, contractors, commercial vendors, and agents
- Federal Government departments and agency personnel, and their contractors and agents

- State government personnel and official representatives of Non-Governmental Organizations (NGO)
- Workstations, guards and firewalls, routers, in-line network encryptors, trusted servers (e.g., database, domain controller, FTP, and WWW), and other infrastructure components. These components must be under the cognizance of humans, who accept the certificate and are responsible for the protection and use of the associated private key

AD Root CA Subscribers include only DOS PKIPO personnel and, when determined by the DOS PKI MA, PKI network or hardware devices.

The Department of State may issue certificates to Subscribers other than employees of the U.S. Government, such as commercial vendors and agents, at the convenience of the Government and without fee, when those Subscribers have a bona fide need to possess a certificate issued by a Department of State CA. The Department of State CA must inform such Subscribers of the stipulations of this policy by including the provisions of Section 9.6.3 in the Subscriber agreements. These Subscribers are under the same policy obligations as those specified for a DOS direct hire.

1.3.9 PKI Sponsors

A PKI Sponsor fills the role of a Subscriber for groups, organizations, disabled personnel, and non-human system components named as public key certificate subjects. PKI Sponsors must be DOS Direct Hires. Where certificates are issued to one of these end entities, the end entity must have a human sponsor who is responsible for carrying out Subscriber duties. For a non-person entity the human Sponsor asserts that the key and certificate will be used in accordance with this policy. The PKI Sponsor works with the CMAs to register the above entities in accordance with Section 3.2.2 and 3.2.3, and is responsible for meeting the obligations of Subscribers as defined throughout this document.

1.3.10 Affiliated Organizations

Subscriber certificates may be issued on behalf of an organization, other than the organization operating the Entity PKI, that has a relationship with the subscriber; this is termed affiliation. The organizational affiliation will be indicated in the certificate. Affiliated Organizations are responsible for verifying the affiliation at the time of certificate application and requesting revocation of the certificate if the affiliation is no longer valid.

1.3.11 Relying Parties

A Relying Party uses a Subscriber's certificate to verify or establish:

- The identity and status of an individual
- The integrity of a digitally signed message
- The identity of the creator of a message
- Confidential communications with the Subscriber

The Relying Party relies on the validity of the binding between the Subscriber's name and public key. 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 Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. For this Certificate Policy, the relying party may be any Entity that wishes to validate the binding of a public key to the name of a federal employee, contractor, or other affiliated personnel.

This CP makes no assumptions or limitations regarding the identity of Relying Parties. While Relying Parties may be Subscribers, Relying Parties are not required to have an established relationship with the DOS PKI CA, FBCA, FCPCA, or another Entity CA.

1.3.12 Other Participants

All CAs operating under this policy require the services of other security and application authorities, such as compliance auditors and attribute authorities. Each CA must identify, in its CPS, the parties responsible for providing such services and the mechanisms used to support these services. Section 5.2 provides more detail on these authorities, services, and mechanisms.

Additional organizations that have a role in PKI operation are:

- The Anti-Virus team, under the Systems Integrity Division, also supports management and operation of the PKI. They provide anti-virus support in the form of up-to-date anti-viral software to all DOS PKI CA servers and RA/LRA workstations.
- Bureau of Diplomatic Security (DS):
  - Establishes and promulgates physical security policies as appropriate to PKI
  - Provides Intrusion Detections System (IDS) monitoring for PKI
  - Takes appropriate investigative, administrative, and disciplinary action when a security violation or compromise is suspected
- Office of Information Assurance (IA):
  - Validates that the PKI meets the security requirements as defined in 12 FAM
  - Conducts Certification and Accreditation activities for the Designated Approving Authority as outlined in Federal Public Key Infrastructure Policy Authority (FPKIPA) Security Control Overlay of NIST Special Publication 800-53 Revision 5 Security Controls for Federal PKI Systems (FPKIPA 800-53 Overlay)
- Information Technology Configuration Control Board (IT-CCB):
  - Approves specification change procedures
  - Defines technical specifications to be implemented by the DOS PKIPO
  - Defines the standard operating procedures for IT changes
- Third Party Compliance Auditors
  - Audit compliance of CPS with governing Certificate Policies

- Audit compliance of PKI operations with the CPS

- IRM
  - Provides networking including basic network security functions such as firewalls
  - Provides general IT/communications support

- Application Owners
  - Provide all necessary information and assistance to support PKI-enabling of their specific application

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Uses

The sensitivity of the information processed or protected using certificates issued by a DOS PKI CA may vary significantly. Relying Parties should 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. Each Relying Party makes this evaluation for its application outside the control of this DOS PKI CP. To provide sufficient granularity, this CP specifies security requirements at five increasing, qualitative levels of assurance: Rudimentary, Basic, Medium, Medium Hardware, and High. The DOS AD Root CA issues at least one High assurance certificate, so the DOS AD Root CA will operate at that level.

All Department of State bureaus that use PKI technology to secure data are subject to the requirements of this policy. DOS requires other agencies that exchange information electronically with Department assets, including those requiring the security of Public Key technology, are subject to the Department's requirements as specified in 12 FAM 600. Each CA asserting this policy must state this requirement in the CPS and inform Subscribers of the limitation.

The level of assurance associated with a public key certificate describes the procedures and controls involved in validating a Subscriber's identity and binding that identity to a public key. It is the responsibility of the Relying Party to assess that level of assurance and determine if it meets their security requirements for some particular use. The level of assurance depends on the proper generation and management of the certificate and associated private keys, in accordance with the stipulations of this policy. Personnel, physical, procedural, and technical security controls contribute to the assurance level of the certificates issued by a certificate management authority or system.

The following table provides a brief description of the appropriate uses for certificates at each level of assurance defined in this CP. These descriptions are guidance and are not binding.

Table 1-5 Certificate Uses

Assurance Level	Appropriate Certificate Uses
Rudimentary	This level provides the lowest degree of assurance concerning identity of the individual. One of the primary functions of this level is to provide data integrity to the digitally signed information. This level is relevant to environments in which the risk of malicious activity is considered low. It is not suitable for transactions requiring authentication, and is generally insufficient for transactions requiring confidentiality, but may be used for the latter where certificates having higher levels of assurance are unavailable.
Basic	This level provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but which are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high. This security level assumes that subscribers are not likely to be malicious.
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. This level of assurance includes the following certificate policies: Medium and Medium Device.
Medium Hardware	This level is relevant to environments where threats to data are high or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk. This level of assurance includes the following certificate policies: Medium Hardware and Medium Device Hardware.
High	This level is reserved for cross certification with government entities and is appropriate for those environments where the threats to data are high, or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk. This level of assurance includes the following certificate policies: High Assurance and Administrator Authentication.

General usage for certificates covered by this policy includes:

- Digital signature services (authentication and data integrity)
- Protection (confidentiality)
- Technical non-repudiation

- Authentication of identity and status with the Department for access control to information systems across the Federal Government

Unless otherwise noted, signatures applied by Subscribers/PKI Sponsors to documentation and communications related to the issuance and lifecycle management of certificates should be digital signatures whenever possible. All signatures applied to documentation and communications related to the issuance and lifecycle management of certificates by RAs and/or other persons in trusted roles must be digital signatures using certificates issued by the appropriate CA at an equivalent or higher assurance level than the transaction signed whenever feasible. All signatures applied by the CA, CSS/OCSP if any, or any other device that is part of the DOS PKI CA infrastructure must use digital signature certificates issued by that CA at the operating assurance level of the CA.

The DOS PKIPO must manage the resulting digitally signed records in accordance with this CP (See Section 5.5) and National Archives and Records Administration (NARA) established records management standards and guidelines applicable to PKI records. For records not directly associated with PKI transactions (e.g., certificate issuance is a PKI transaction), it is the responsibility of the implementer to ensure that the digital signatures can be validated for the full records retention period of the signed statements beyond the retention requirements identified in Table 5-5.

1.4.2 Prohibited Certificate Uses

Subscribers must not use DOS PKI certificates to conceal an unauthorized act as specified in Federal law or Department of State regulation (see 12 FAM 590). Examples of such actions include, but are not limited to, the following:

- Use of PKI certificates, especially in conjunction with a DOS-issued PIV card, to gain unauthorized access to a federal facility, information system, or electronic data (e.g., Privacy information), or to enable others to gain such access
- Use of PKI certificates to facilitate and/or hide an unauthorized action, such as:
  - Transfer information to an unauthorized individual
  - Generate income for oneself or for an organization
  - View sexually explicit material, gamble, or for the purposes of conducting unlawful or malicious activities
  - Negatively affect the integrity, accessibility, and/or confidentiality of the Department’s cyber infrastructure

The Department specifically prohibits such uses of PKI regardless of whether the use is during or outside normal work hours, whether use occurs on or off U.S. Government premises, or whether the use occurs within or outside the United States.

Each CA asserting this policy must state this requirement in the CPS and inform Subscribers of these usage limitations. All Department of State bureaus, offices, and posts that use PKI technology are subject to the requirements of this policy. Other agencies that exchange

information electronically with Department assets using Public Key technology are subject to the Department's requirements.

1.4.3 Wildcard Certificates

A wildcard certificate is a certificate issued to a device that contains the wildcard designator (*) in either the common name (CN) in the Subject field or the subjectAltName (SAN) extension, or both. Only device SSL or TLS certificates that assert serverAuth in the extended Key Usage (EKU) extension may contain a wildcard designator (*). A wildcard certificate allows multiple devices to share the same public-private key pair.

The DOS PKI CPS must identify the DOS PKI CAs authorized to issue wildcard certificates.

1.5 POLICY ADMINISTRATION

1.5.1 Organization Administering the Document

The DOS PKI MA is responsible for all aspects of this DOS PKI CP.

1.5.2 Contact Person

Direct questions regarding this CP to Chief, Systems Integrity Division, as the DOS PKI MA, at the following address:

U.S. Department of State Annex SA-7B
Attn: IRM/FO/ITI/SI
7958 Angus Court
Springfield Virginia, 22153
(703) 866-7265

1.5.3 Person Determining Certification Practices Statement Suitability for the Policy

Certification Practices Statements for each DOS PKI CA must conform to the DOS PKI Certificate Policy. The Division Chief, Systems Integrity Division, as the DOS PKI PMA, must determine the suitability of any CPS to this policy. In each case, the DOS PKI PMA must base the determination of suitability on an independent compliance auditor's results and recommendations. See Section 8 for further details.

1.5.4 CPS Approval Procedures

The DOS PKI OA must submit the CPS for each DOS PKI CA, and the results of an audit of its compliance with the DOS PKI CP, through the DOS PKI MA to the DOS PKI PMA for approval. The DOS PKI PMA must make the final determination if the CPS complies with the DOS PKI CP for a given level of assurance. The DOS PKI PMA accepts or rejects the CPS. If rejected, the DOS PKI OA must resolve the identified issues and resubmit the revised CPS to the DOS PKI PMA for approval. The CPS for each DOS PKI CA must meet all requirements of the DOS PKI CP before the CA commences operations.

The DOS PKI PMA may grant policy waivers only to meet urgent, unforeseen operational requirements. When the DOS PKI PMA grants such a waiver, the DOS PKI MA must notify Relying Parties of said waiver, and:

- Implement a permanent change to the DOS PKI CP to address the requirement, or
- Place a specific time limit, not to exceed one year, on the waiver.

The DOS PKI MA, through the DOS PKI PMA, must notify the FPKIPA of the waiver, and provide information regarding the specific provision waived, the rationale for granting the waiver, and either an estimate of the time needed to resolve the situation or a request for re-cross certification based on the permanent change made to the DOS PKI CP.

1.6 DEFINITIONS AND ACRONYMS

See Appendix B for acronyms and Appendix C for definitions.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

The DOS PKIPO must use only repository mechanisms and procedures designed to ensure CA certificates and CRLs are available for retrieval 24 hours a day, 7 days a week, with a minimum of 99% availability overall per year and scheduled down-time not to exceed 0.5% annually[9].

2.2 PUBLICATION OF CERTIFICATION INFORMATION

2.2.1 Publication of Certificates and Certificate Status

The DOS PKIPO must operate repositories to support DOS PKI CA operations. The location of any publication will be one that is appropriate to the certificate-using community, and in accordance with the total security requirements of the Department. The DOS PKIPO must ensure interoperability with the FBCA and/or FCPCA repository.

The DOS PKI CA infrastructure will serve as the primary repository of information for Subscribers and Relying Parties. For all DOS PKI CAs, this repository is the DOS directory infrastructure operated by IRM/OPS// Enterprise Network Management (ENM).

The DOS PKIPO web site, https://usdos.sharepoint.com/sites/irm-fo/iti/si/iib/pki/sitepages/home.aspx, serves as the primary repository to publish information. Network directories and all other repositories used to disseminate relevant information will:

- Maintain availability necessary to distribute current certificate information in a manner consistent with the posting and retrieval stipulations of this CP Section and the appropriate CA CPS
- Implement access controls and communication mechanisms on all CA repositories to provide sufficient protection as described in Section 5.1.2.

The DOS PKIPO may use a variety of mechanisms for posting information into a repository as required by this CP. These mechanisms at a minimum must include:

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

CA and End Entity certificates must contain valid Uniform Resource Identifiers (URIs) that are publicly accessible, for the purposes of certification path building and for revocation checking.

[9] Where repository systems are distributed, the availability figures apply to the system as a whole, rather than each component; and availability targets exclude network outages.

The DOS PKI must publish all CA certificates it issues in a file available via a publicly accessible HTTP URI. This URI must be asserted in the SIA extension in all valid certificates issued to the CA. The file must be a certs-only Cryptographic Message Syntax file that has an extension of .p7c.

Except for self-signed certificates, all CA certificates must be published by the Subject CA in a file available via a publicly accessible HTTP URI. This URI must be asserted in the AIA extension in all valid certificates issued by the Subject CA. The file must be:

- A certs-only Cryptographic Message Syntax file that has an extension of .p7c, or
- A single DER encoded certificate that has an extension of .cer.

The certs-only Cryptographic Message Syntax format is preferred as it allows flexibility for inclusion of multiple certificates.

CAs must publish the latest CRL covering all unexpired certificates via a publicly accessible HTTP URI until such time as all issued certificates have expired. This URI must be asserted in the CRL distribution point extension of all certificates issued by that CA, except for OCSP responder certificates that include the id-pkix-ocsp-nocheck extension.

When implemented, a CSS provides status information about certificates on behalf of a CA through on-line transactions in the form of a delegated Online Certificate Status Protocol (OCSP) service, as described in [RFC 6960], to provide on-line status information for Subscriber certificates via a publicly accessible HTTP URI in the AIA extension. The operations of the OCSP service are within the scope of this CP.

Each Root and subordinate CA in the Department of State PKI must publish certificates issued or received, and status information, such that it is available over the OpenNet Plus[10] network or other such networks appropriate to a particular "community of interest" and that includes the following:

- Issued certificates that reference this Certificate Policy and have the Key Encipherment bit set in the Key Usage attribute
- All CRLs (optionally, each CA may also utilize an OCSP responder)
- The applicable CA certificates to validate a Subscriber certificate
- All CA certificates issued by or to the CA and CRLs issued by the CA in a repository that is publicly accessible through all URI references asserted in valid certificates issued by that CA

2.2.2 Publication of CA Information

The DOS PKIPO must publish information concerning the DOS PKI necessary to support its use and operation.

[10] The OpenNet Plus network has Internet access.

A copy of the current DOS PKI CP must be posted on the following publicly available web site https://pkaps.pki.state.gov/pkiinfo/.

A copy of the FCPF CP is publicly available on the FPKIPA website (https://www.idmanagement.gov).

The DOS PKIPO will not publish the CPS for any DOS PKI CA as a public document due to the potential sensitivity of operational and security information contained herein. Distribution of the CPS for any DOS PKI CA is limited to individuals responsible for the management, operations, and audit of the DOS PKI on a need-to-know basis.

Cross-certified CAs and other Relying Parties may request a copy of the CPS for any DOS PKI CA from the DOS PKI MA, whose contact information is provided in Section 1.5.2 of this CP. The DOS PKI MA will review the requests to determine if a copy of the CPS or a redacted copy of the CPS will be provided or not and notify the requester.

A copy of the most recent DOS PKI Annual Compliance Audit Letter must be available on the following publicly available web site https://pkaps.pki.state.gov/pkiinfo/.

The DOS PKI MA must send this DOS PKI CP and subsequent revised DOS PKI CPs to CMAs that assert this policy within 5 business days of approval. The CMAs will notify Subscribers of any approved changes to the Certificate Policy that directly affect them or their PKI-related responsibilities. (See Section 9.12.2)

2.2.3 Interoperability

Where the DOS PKI CAs publish certificates and CRLs in directories, the directories must use standards-based schemas whenever possible for directory objects and attributes in accordance with technical guidance from the FPKI Management Authority. CA and End Entity certificates must only contain valid URIs that are accessible by relying parties.

2.3 TIME OR FREQUENCY OF PUBLICATION

The DOS PKI PMA must make this CP and any subsequent changes to this CP available within 30 days of approval on the following publicly available web site https://pkaps.pki.state.gov/pkiinfo/.

The appropriate DOS PKI CA will publish certificates following user acceptance as specified in Section 4.4 and proof of possession of private key as specified in Section 3.2.1. Section 4.9 specifies publication requirements for CRLs. The CA must publish all information normally published in the repository promptly after such information becomes available. Each PKI CA CPS must specify time limits within which it publishes various types of information.

2.4 ACCESS CONTROLS ON REPOSITORIES

Each DOS PKI CA must adequately protect any repository information not intended for public dissemination or modification; and must not make Subscriber certificates automatically available on any public facing repository.

The appropriate CPS must detail the information in the repository that must be exempt from automatic availability, and to whom and the conditions under which the DOS PKI MA may make restricted information available via direct and/or remote access.

3. IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

This CP establishes requirements for both subject distinguished names and subject alternative names.

CA certificates must contain a non-null subject Distinguished Name (DN). All RA certificates must include a non-NULL subject DN. This CP does not restrict the types of names that can be used.

The table below specifies the naming requirements that apply to each level of assurance.

Table 3-1 Naming Requirements

Assurance Level	Naming Requirements
Rudimentary	Non-Null Subject Name, or Null Subject Name if Subject Alternative Name is populated and marked critical
Basic	Non-Null Subject Name, and optional Subject Alternative Name if marked non-critical
Medium (all policies)	Non-Null Subject Name, and optional Subject Alternative Name if marked non-critical
High	Non-Null Subject Name, and optional Subject Alternative Name if marked non-critical

3.1.1.1 Subject Names

Certificates issued to Subscribers must include distinguished names that are comprised of a base distinguished name (Base DN) and additional relative distinguished names (RDNs). Base DNs must be in either of two forms: a geo-political name or an Internet domain component name.

All geo-political distinguished names must use the following Base DN:

- C=US, o=U.S. Government, ou= department, [ou=*structural_container*]

The organizational unit department is used to specify the federal entity that employs the Human Subscriber or owns the device.

Distinguished names based on Internet domain component names must use the following Base DN:

- dc=gov, dc=org0, [dc=org1], …, [dc=orgN], [o=organization], [ou=*structural_container*]

At a minimum, the org0 domain component must appear in the Base DN. The org1 to orgN domain components appear, in order, when applicable, and are used to specify the federal entity that employs the Human Subscriber or owns the device.

The additional organizational unit *structural_container* in either the geo-political or Internet domain Base DN form is permitted to support local directory requirements, such as differentiation between Human Subscribers and Device Subscribers. This organizational unit shall not be employed to further differentiate between subcomponents within an agency.

The distinguished name of the Human Subscriber must include a common name (CN) using one of the following formats:

- Base DN, CN=nickname lastname
- Base DN, CN=firstname initial. lastname
- Base DN, CN=firstname initial lastname
- Base DN, CN=firstname middlename lastname
- Base DN, CN=lastname.firstname.middlename

In the first common name format, nickname may be the Human Subscriber's first name, a form of the first name, middle name, or pseudonym (e.g., Jack) by which the Subscriber is generally known. A generational qualifier, such as "Sr." or "III", or agency specific identifiers (e.g., CN=Smith.Johnathon.Paul.1234567890) may be appended to any of the common name formats specified above.

Additional certificate qualifiers may be appended to the common name in order to provide additional context to the certificate's intended usage. The qualifier must be preceded by a space followed by a hyphen (e.g., CN=Johnathon P. Smith -Sign).

Distinguished names assigned to federal contractors and other affiliated persons must follow one of the name forms identified above with (affiliate) appended to the end of the common name (e.g., CN=Johnathon P. Smith (affiliate)).

The CA may supplement any of the distinguished name forms for Human Subscribers specified in this section by including a dnQualifier, serial number, or user id. When any of these are included, they may appear:

- as part of a multi-valued RDN with the common name, or
- as a distinct RDN that follows the RDN containing the common name

Role-based and Group certificates may be issued under any non-PIV human subscriber policy.

For Role-based certificates, the common name specifies the role, as follows:

- CN=role [, department]

Where the [department/agency] is implicit in the role (e.g., Secretary of State), it should be omitted. Where the role alone is ambiguous (e.g., Chief Information Officer) the

department/agency must be present in the common name. The organizational information in the common name must match that in the organizational unit attributes.

For Group certificates, the common name specifies the group, as follows:

- CN=group [, department]

The subjectName DN in a Group certificate must not imply that the subject is a single individual, e.g., by inclusion of a human name form.

A Device Subscriber name must be a unique name for the device and must not take the form of a Human Subscriber name. Device Subscriber distinguished names must take the following form:

- Base DN, CN=device name

where device name is a descriptive name for the device.

When id-fpki-common-pivi-cardAuth is asserted, the certificate's subject distinguished name must take the following form:

- Base DN, serialNumber=UUID

This CP does not restrict the subject distinguished names of CA certificates and Delegated OCSP Responder certificates. However, CA certificates and Delegated OCSP Responder certificates must have subject distinguished names. CA and Delegated OCSP Responder certificate distinguished names may be either a geo-political name or an Internet domain component name. Geo-political distinguished names must be composed of any combination of the following attributes: country; organization; organizational unit; and common name. Internet domain component names are composed of the following attributes: domain component; organizational unit; and common name.

CA subject distinguished names may or may not include a common name, for example:

- Base DN, OU=Certification Authorities, OU=Department CA

If included, the common name in the CA certificates should describe the issuer, such as:

- Base DN, OU=Certification Authorities, CN= Department of State AD High Assurance CA

3.1.1.2 Subject Alternative Names

Subscriber certificates that contain id-kp-emailProtection in the EKU must include a subject alternative name extension that includes a rfc822Name.

3.1.1.3 Wildcard Certificate Names

For Device Subscriber certificates that assert serverAuth in the Extended Key Usage, wildcard domain names are only permitted in the dNSName value if all sub-domains covered by the wildcard fall within the same application, cloud service, or system boundary within the scope of the sponsoring organization.

For wildcard certificates, the wildcard designator (*) may be included in the Common Name (CN) in the Subject field, or the subjectAltName (SAN) extension, or both

3.1.2 Need for Names to Be Meaningful

Names used within the Department of State must identify the person or object to which assigned in a meaningful way.

The common name in the distinguished name must represent the Subscriber in a way that is easily understandable for humans. For Human Subscribers, this will typically be a legal name.

The CMA must ensure that an affiliation exists between the Subscriber and any organization identified by any component of any name in its certificate. A CMA who uses DNs will coordinate with such authority to determine the proper elements for a given Subscriber.

Any CA asserting this policy must only sign certificates with subject names from within a namespace approved by the DOS PKI MA and Department Naming Authority.

When DNs are used, the directory information tree must accurately reflect organizational structures.

In addition, the common name must represent the Subscriber in a way that is easily understandable for humans.

When DNs are used, the common name must respect name space uniqueness requirements and must not be misleading. This does not preclude the use of pseudonymous certificates as defined in Section 3.1.3. The subject name in CA certificates must match the issuer name in certificates issued by the CA, as required by [RFC 5280].

Wildcard certificates must not have the wildcard designator immediately to the left of an agency or organization name (e.g., *.[agency].gov).

The name space of the wildcard certificate must be specific to restrict the use of the certificate to the system or set of systems designated for a single application or service.

3.1.3 Anonymity or Pseudonymousness of Subscribers

CA certificates must not contain anonymous or pseudonymous identities.

The DOS PKI AD Root CA must not issue anonymous certificates. CA certificates issued by the AD Root CA must not contain anonymous or pseudonymous identities.

Subordinate CAs may issue pseudonymous certificates to support internal operations.

DNs in subscriber certificates issued by CAs may contain a pseudonym (such as a large number) as long as name space uniqueness requirements are met.

CAs may issue Role-based or Group certificates that identify subjects by their organizational roles. Each identified 'role' or 'group' must meet name space uniqueness requirements.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting name forms will use the appropriate standard:

- ITU-T X.501 for interpreting distinguished name forms
- IETF RFC 5322 for interpreting e-mail addresses
- Appropriate IETF RFCs for URL and IP addresses, etc.

The applicable certificate profile (see Section 7.1), as established by the Naming Authority, will contain the rules for interpreting that name form. The CPS must identify the Naming Authority.

3.1.5 Uniqueness of Names

The DOS Naming Authorities must enforce name uniqueness across the Department. Wherever practical, AD CAs must use X.500 distinguished names allocated by the Department Naming Authority. DOS PKI CAs and RAs must enforce name uniqueness within the authorized X.500 name space. When other name forms are used, they too must be allocated such that name uniqueness is ensured for certificates issued by that CA. DOS AD CAs must use distinguished names allocated by the Department Naming Authority suitable for the AD operating system.

Each DOS PKI CA will unambiguously identify each object in the naming hierarchy for the certificate repository using DNs. The DOS Naming Authorities or CAs will ensure that a DN, once assigned, remains unique for the lifetime of the PKI, and will not re-use that name to identify a different entity. Name uniqueness is not violated when multiple certificates are issued to the same entity. For distinguished names, name uniqueness is enforced for the entire name rather than a particular attribute (e.g., the common name).

When other name forms are used, CMAs must allocate them, such that name uniqueness is assured across the Department. Each DOS PKI CA must document permitted name forms in its CPS; how the CAs and RAs will interact with the Department Naming Authority; and how CMAs will allocate names within the Subscriber community to guarantee name uniqueness among current and past Subscribers.

The CMA must investigate and if necessary recommend the correction for any name collisions brought to its attention. The CMA must coordinate with and defer to the Naming Authority where appropriate.

Where there is a certificate with a wildcard designator in the CN, the PKI must not issue any other certificate with a CN that overlaps or is a subset of that namespace.

Wildcard Domain Names are permitted if all sub-domains covered by the wildcard fall within the same application, cloud service, or system accreditation boundary within the scope of the sponsoring organization.

Wildcards must not be used in subdomains that host more than one distinct application platform. The use of third-level Agency wildcards, (e.g., *.[agency].gov), must be prohibited to reduce the likelihood that a certificate will overlap multiple systems or services. Third level wildcards are permitted for DNS names dedicated to a specific application (e.g., *.[application_name].gov, or *.[application_name].sbu).

Before issuing a serverAuth certificate containing a wildcard, the CA must ensure the sponsoring organization has a documented procedure for determining that the scope of the certificate does not now and will not infringe on other agency applications.

3.1.6 Recognition, Authentication, and Role of Trademarks

The CMA must investigate and if necessary recommend the correction for any trademark name collisions brought to its attention. The CMA must coordinate with and defer to the Naming Authority where appropriate. The CMA will communicate resolutions to all interested parties.

Consistent with Federal Policy, DOS PKI CAs will not knowingly use, or permit the use of, trademarks in names unless the subject has the rights to use that name.

3.2 INITIAL IDENTITY VALIDATION

Certificate applicants must communicate application requests for certificates to an authorized RA or LRA via a trustworthy process, but generally in person. An authorized RA, equipped with Registration Authority hardware and software, may communicate authorizations to issue certificates directly to the supporting CA electronically, provided all communication is secure. An LRA, who is not equipped with Registration Authority hardware and software, must transmit authorization requests to issue certificates to the appropriate RA by secure means (i.e., digitally signed electronic means, via diplomatic pouch or registered mail, or in person).

3.2.1 Method to Prove Possession of Private Key

In the case where the CMA generates the key directly on the Subscriber's token, or in a key generator that benignly transfers the key to the Subscriber's token, then the end-entity is presumed to be in possession of the private key at the time of generation or transfer and proof of possession is not required. If the user is not in possession of the token during key generation, the CMA must deliver the token to the Subscriber via an accountable method (see Section 6.1.2). The CMA must obtain written or electronic (via the PKI system) acknowledgment of receipt from the Subscriber within 21 days of shipment or must revoke any certificates issued to that Subscriber. The CMA must deliver activation data for the private keys within the token or module to the Subscriber through a separate, secure communication unless the CMA delivers the token or module in person.

When the CMA delivers keyed hardware tokens to Subscribers, they must accomplish delivery in a way that ensures that they provide the correct tokens and activation data to the correct people. The CMA must maintain a Subscriber token receipt validation record. When any mechanism that includes a shared secret (e.g., a passphrase or PIN) is used, the mechanism must ensure that the applicant and the CMA are the only recipients of this shared secret.

In those cases where the Subscriber causes the system to generate keys (e.g., remote emergency renewal), the Subscriber is required to prove possession of the private key that corresponds to the public key in the certificate request to the CMA.

In the case where key generation is performed under the CA or RA's direct control, proof of possession is not required (e.g., key management certificates generated in a system allowing key escrow).

3.2.2 Authentication of Organization Identity

A DOS PKI CA may issue certificates directly in the name of an organization rather than an individual for those functions and applications performed on behalf of the organization. The CMA must authenticate the identity of any organization that appears as a component of a subject name appearing in a certificate issued by the CA before processing the certificate application. Any organization requesting a certificate must have a PKI Sponsor to accept the obligations of the organization. This section pertains only to the authentication and naming of an organization as the subject in a certificate.

Requests for certificates in the name of an organization or group must include the necessary identifying data of the Sponsor, the group or organization name, address, and documentation of the existence of the organization. This information will include but is not limited to the following:

- Organization identification and authorization
- Certificate Authority public keys (for subordinate and cross-certified CAs)
- Contact information to enable the CMA to communicate with the PKI Sponsor as required

The CMA must verify this information, in addition to the authenticity and authorization of the requesting PKI Sponsor, authenticate the validity of any authorizations to be asserted in the certificate, and verify the source and integrity of the data collected to an assurance level commensurate with the certificate assurance level requested. The CPS will specify acceptable measures for authenticating both the organization and PKI Sponsor's identity and authorizations.

The CMA must also include his or her own identity information and authentication declaration as outlined in Section 3.2.3. The PKI Sponsor must present information sufficient for registration at the level of assurance requested, for both himself or herself and the non-human Entity (i.e., organization or group) requesting a certificate, and must authenticate this information in-person as prescribed in Section 3.2.3.

Before issuing subscriber certificates on behalf of an affiliated organization, the issuing CA must verify the authority of requesting representatives.

For specific requirements for verification of wildcard certificates, see Section 3.2.3.4.

3.2.3 Authentication of Individual Identity

For each certificate issued, the CA must authenticate the identity of the individual requestor.

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

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

3.2.3.1 Authentication of Human Subscribers

For Subscribers (including all RAs/LRAs and PKI Sponsors of organizations, components, and minors or others not legally competent), the CMA must ensure that the applicant's identity information is verified in accordance with this CP, the applicable CPS, and all applicable MOAs. The CMA must ensure that the applicant's identity information and public key are adequately bound. For each assurance level, the applicant must meet the minimum set of requirements identified in this section. A CMA may use mechanisms of equivalent or stronger assurance if documented in their CPS. The appropriate DOS PKI CA CPS will specify the acceptable procedures for authenticating a Subscriber's identity.

The CMA must record the process followed for each certificate. Process information must depend upon the certificate's level of assurance and must be addressed in the applicable CPS. In addition, the documentation and authentication requirements must vary depending upon the level of assurance. At a minimum, process documentation and authentication requirements must include the following, depending on the level of assurance for issuance of each certificate:

- Identity of the applicant
- Identity of the person performing the identification and either:
  - A signed declaration by that person that he or she verified the identity of the applicant against official government-issued photo ID as required using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law, or
  - An auditable record linking the authentication of the person performing the identification to their verification of each Applicant.

- If in-person or supervised remote[11] identity proofing is done, a unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s)
- If electronic authentication is done, a unique identifying number(s) from the signature or authentication certificate must be retained (e.g., certificate, serial number, thumbprint, SKI, public key, etc.)
- The date of the verification, and either:
  - An auditable record indicating the applicant accepted the certificate; or
  - A declaration of identity signed by the applicant using a handwritten signature or appropriate digital signature (see Practice Note) and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.

The table below summarizes the identification requirements for each level of assurance.

Table 3-2 Identification Requirements

Assurance Level	Identification Requirements
Rudimentary	No identification requirement; applicant may apply and receive a certificate by providing his or her e-mail address.
Basic	Identity may be established by in-person proofing before a Registration Authority or Trusted Agent; or remotely verifying information provided by applicant including ID number and account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, date of birth, address and other personal information in records are consistent with the application and sufficient to identify a unique individual. Address confirmation: a) Issue credentials in a manner that confirms the address of record supplied by the applicant; or b) Issue credentials in a manner that confirms the ability of the applicant to receive telephone communications at a number associated with the applicant in records, while recording the applicant's voice.

[11] The minimum requirements associated with supervised remote identity proofing are described in NIST SP 800-63A, *Digital Identity Guidelines.*

Table 3-2 Identification Requirements

Assurance Level	Identification Requirements
Medium (all policies)	Identity must be established by in-person or supervised remote proofing before the Registration Authority, Trusted Agent or an entity certified by a State or Federal Entity as being authorized to confirm identities; information provided must be verified to ensure legitimacy. A trust relationship between the Trusted Agent and the applicant which is based on an in-person antecedent may suffice as meeting the in-person identity proofing requirement. Credentials required are one Federal Government-issued Picture I.D., one REAL ID Act compliant picture ID[12], or two Non-Federal Government I.D.s, one of which must be a photo I.D. Any credentials presented must be unexpired.
High	Identity established by in-person appearance before the Registration Authority or Trusted Agent; information provided must be checked to ensure legitimacy. Credentials required are either one Federal Government-issued Picture I.D., one REAL ID Act compliant picture ID., or two Non-Federal Government I.D.s, one of which must be a photo I.D. (e.g., Driver's License).

A CPS must indicate what actors, roles, responsibilities, and activities are leveraged when relying on in-person antecedent to support identity proofing (e.g., agreement with a professional organization to use a member identification number and associated provided point of contact information as antecedent, or electronic authentication using a medium or above certificate being traced back to the initial identity proofing event).

For All Levels: As an alternative to presentation of identification credentials, the CMA may use other mechanisms of equivalent or greater assurance (such as comparison of biometric data to identities pre-verified to the standards of this policy and obtained via authenticated interaction with secured databases). If databases or other sources are used to confirm applicant attributes, then these sources and associated information sent to the DOS PKI AD Root CA or subordinate CA must require:

- When information is obtained through one or more information sources, an auditable chain of custody must be in place
- All data received must be protected and securely exchanged in a confidential and tamper evident manner and protected from unauthorized access.

If an applicant is unable to perform face-to-face, either in-person or supervised remote, registration (e.g., a network device), the applicant may be represented by a trusted person already

[12] REAL ID Act compliant IDs are identified by the presence of the DHS REAL ID star

issued a digital certificate by the PKI. The trusted person will present information sufficient for registration at the level of the certificate being requested, for both himself/herself and the applicant for whom the trusted person is representing.

For Medium and High Assurance: The CMA must establish identity no more than 30 days before initial certificate issuance. Before enabling the applicant's certificate, the CMA must personally verify the applicant's identity. Minors and others not legally competent to provide face-to-face registration information alone must be accompanied by a person already certified by the DOS PKI (i.e., a Sponsor), who will present information sufficient for registration at the level of the certificate being requested, for himself or herself, and the accompanied person. Persons not physically capable of providing face-to-face registration information must be proxied by a person already certified by the DOS PKI, who will present information sufficient for registration at the level of the certificate requested, for both himself or herself and the person unable to appear himself or herself.

For the Basic and Medium Assurance Levels: An Entity certified by a State or Federal Entity as being authorized to confirm identities may perform in-person authentication on behalf of the RA/LRA and may be considered a Trusted Agent. The certified Entity forwards the information collected from the applicant directly to the RA/LRA in a secure manner. Packages secured in a tamper-evident manner by the certified Entity satisfy this requirement; other secure methods are also acceptable. Such authentication does not relieve the RA/LRA of responsibility to verify the presented data.

In the event an applicant is denied a credential based on the results of the identity proofing process, a mechanism for appeal or redress of the decision must be provided.

3.2.3.2 Authentication of Human Subscribers for Role-Based Certificates

The DOS CAs may issue Role-based digital signature and key management certificates to a subset of human Subscribers. These certificates identify a specific role on behalf of which the Subscriber is authorized to act rather than the Subscriber's name. DOS issues these certificates in the interest of supporting accepted business practices. For pseudonymous Role-based certificates that identify certificate subjects by their organizational roles, the RA/LRA must validate that the individual requesting the Role-based certificate either holds that role or has been delegated the authority to sign on behalf of the role. Role-based digital signature certificates are used in situations where non-repudiation is required or desirable. DOS CAs shall issue Role-based certificates only to persons holding a currently valid DOS-issued PIV credential.

In case a Subscriber for Role-based certificate changes, the new Subscriber/PKI Sponsor must review the status of each holder of such a certificate to ensure that they are still authorized to act in that role and are required to have certificates. The new Subscriber/PKI Sponsor must notify a RA/LRA of the change in sponsorship and re-affirm the ongoing need for such certificates via an email digitally signed using their DOS-issued PIV credential and/or in-person. The applicable CPS must describe procedures to ensure that accountability is maintained; and describe the procedures for modification, if any, in accordance with Section 4.8.

Role-based certificates must not be shared but must be issued to individual Subscribers and protected in the same manner as individual certificates. DOS CAs may issue certificates for a specific role to multiple Subscribers, but the key pair for each certificate must be unique to each individual Role-based certificate. Roles, for which a RA may issue Role-based certificates, are limited to those that uniquely identify a specific individual within DOS by his/her role (e.g., *Chief Information Officer* is a unique individual; *Program Analyst* is not a unique role).[13]

The issuing Subordinate DOS PKI CA and/or RAs/LRAs must record the information identified in Section 3.2.3.1 for the Sponsor associated with the role before issuing a Role-based certificate. The RA/LRA must validate the identity of the Sponsor by requiring the Sponsor to submit a request for the issuance of the Role-based certificate(s) that is digitally signed using the Sponsor's currently valid DOS-issued PIV credential. If the Sponsor requests the issuance of the Role-based certificates to additional Subscribers, the RA/LRA or the CMS must verify that each of the Subscribers have a currently valid DOS-issued PIV credential. The procedures for issuing Role-based certificates must comply with all other stipulations of this CP (e.g., key generation, private key protection, Subscriber obligations).

3.2.3.3 Authentication of Human Subscribers for Group Certificates

Normally, DOS CAs must issue a certificate to a single Subscriber. For cases where there are several entities acting in one capacity, and where non-repudiation for transactions is not required, a certificate may be issued that corresponds to a private key that is shared by multiple Subscribers. Subordinate DOS PKI CAs and/or RA/LRAs must record the information identified in Section 3.2.3.1 for a Sponsor, from the organization's Information Systems Security Office or equivalent, as well as for the subordinate PKI CA CMA, before issuing a Group certificate. The RA/LRA must validate the identity of the Sponsor by requiring the Sponsor to submit a request for the issuance of the Group certificate that is digitally signed using the Sponsor's currently valid DOS-issued PIV credential.

In addition to the authentication of the Sponsor, the RA/LRA must perform the following procedures for members of the group:

- The Information Systems Security Office or equivalent must be responsible for ensuring control of the private key, including maintaining a list of Subscribers who have access to use of the private key, and accounting for which Subscriber had control of the key at what time
- The Information Systems Security Office or equivalent must ensure that only Subscribers that have a currently valid DOS-issued PIV credential are allowed access to use the private key
- The *subjectName* DN must not imply that the subject is a single individual, e.g. by inclusion of a human name form

[13] When determining whether a role-based certificate is warranted, consider whether the role carries inherent authority beyond the job title. Role-based certificates may also be used for individuals on temporary assignment, where the temporary assignment carries an authority not shared by the individuals in their usual occupation, for example: "*Shift Lead, Security Operations Center*".

- The list of those with access to the shared private key must be provided to, and retained by, the applicable CA or its designated representative
- The procedures for issuing tokens for use in shared key applications must comply with all other stipulations of this CP (e.g., key generation, private key protection, and Subscriber obligations)
- Group certificates must be issued only to groups under the Sponsor's control.

In case a human Sponsor changes, the new Sponsor must review the status of each group certificate under his/her sponsorship to ensure that it is still authorized to receive and required to have certificates and must notify the CMA of the change in sponsorship and re-affirm the information outlined above via digitally signed email and/or in-person. The applicable CPS must describe procedures to ensure that certificate accountability is maintained.

3.2.3.4 Authentication of Devices

Some computing and communications components (routers, firewalls, servers, etc.) and software applications will be named as certificate subjects. In such cases for all assurance levels, the component must have a human PKI Sponsor who is affiliated with the DOS. The Sponsor is responsible for the security of the private key and for providing the following registration information as prescribed in the applicable DOS PKI CA CPS.

In the case of computing and communications components (equipment), this information shall include but is not limited to the following:

- Equipment or application organizational ownership and authorization to request certificates
- Equipment identification (e.g., serial number) or service name (e.g., DNS name) or unique software application name
- Equipment or software application public keys
- Equipment or software application authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the CA or RA to communicate with the Sponsor when required, and acceptance of sponsorship responsibilities

The CMA must authenticate the validity of any authorizations asserted in the certificate and must verify source and integrity of the data collected to an assurance level commensurate with the certificate assurance level requested. For certificates issued at the *mediumDevice* or *mediumDeviceHardware* policy, the CMA must verify registration information for the device/application and the PKI Sponsor commensurate with the Medium assurance level. The CMA must also include his or her own identity information and authentication declaration as outlined in Section 3.2.3.1. The PKI Sponsor will present information sufficient for registration at the level of assurance requested, for both himself or herself and the non-human Entity (e.g., equipment, groups) requesting a certificate. The PKI Sponsor must authenticate this information in person and/or via a digitally signed email to the CMA using the Sponsor's previously issued

DOS PKI certificate asserting the same or higher level of assurance as that being requested, as prescribed in Section 3.2.3.1.

The registration information must be verified to an assurance level commensurate with the certificate assurance level being requested. For certificates that assert a certificate policy mapped to the id-fpki-certpcy-mediumDevice or id-fpki-certpcy-mediumDeviceHardware policies, registration information must be verified commensurate with the Medium assurance level. Acceptable methods for performing this authentication and integrity checking include, but are not limited to the following:

- Verification of digitally signed messages sent from the Sponsor (using certificates of equivalent or greater assurance than that requested)
- In person or supervised remote registration by the Sponsor, with the identity of the Sponsor confirmed in accordance with the requirements of Section 3.2.3.1

Component certificates must be issued only to devices/applications under the Sponsor's control, or where the Sponsor has delegated to an authorized administrator for the device/application the responsibility to protect the device/application's private key and to ensure that the device/application's certificate is only used for authorized purposes. In case a human Sponsor changes, the new Sponsor must review the status of each component certificate under his/her sponsorship to ensure that it is still authorized to receive and required to have certificates and must notify the CMA of the change in sponsorship and re-affirm the information outlined above via digitally signed email and/or in-person. The applicable CPS must describe procedures to ensure that certificate accountability is maintained. See Section 9.6.3 for Subscriber responsibilities.

Requirements specific to wildcard certificates:

Only device SSL or TLS certificates that assert serverAuth in the EKU extension may contain a wildcard designator (*). The authorized human PKI Sponsor must submit the request for a wildcard certificate, identifying the system or device, and providing other required information, to an authorized RA.

For wildcard certificates, the RA must verify:

- The business and technical justification that necessitates the use of the wildcard certificate.
- The approved existence of the system or device
- The identity of the Sponsor via a DOS-issued signature certificate, issued at mediumHardware or above, on a PIV Card (preferred), a Secure Network Access with PKI (SNAP) smart card, or YubiKey token
- The authority of the PKI Sponsor to request a system or device wildcard certificate
- The authority of the PKI Sponsor to control and manage the wildcard namespaces
- The entire wildcard namespace is under the control of the PKI Sponsor, and
- Any attributes asserted by the system or device wildcard certificate.

For wildcard certificates, the RA must sign a declaration acknowledging that they have verified the identity and any attributes contained in the certificate in accordance with this policy.

For wildcard certificates, the RA must vet the Request against all requirements, document and report the results to the DOS PKI PM. For requests for wildcard certificates for publicly trusted DOS servers the RA must recommend to the DOS PKI PM whether the certificate should be issued by a DOS PKI CA authorized to issue wildcard certificates, or by a trustworthy commercial PKI service. The RA must recommend approval/disapproval of the request.

For wildcard certificates, the DOS PKI PM must approve or disapprove the Request. If approved, the RA must complete the wildcard certificate issuance process as approved, i.e.:

- By issuing the requested certificate from a DOS PKI CA authorized to issue wildcard certificates, or
- By providing guidance to the PKI Sponsor to obtain the certificate from a trusted commercial PKI service provider.

The PKI Sponsor must be accountable for the system or device wildcard certificate and must acknowledge and accept overall responsibility for the use of the system or device wildcard certificate and protection of all copies of the associated private key.

3.2.4 Non-verified Subscriber Information

Except for the rudimentary assurance level, all Subscriber information included in certificates must be verified.

3.2.5 Validation of Authority

For cross certification, the DOS PKI OA must validate the representative's authorization to act in the name of the organization and include such verification in the recommendation through the DOS PKI MA to the DOS PKI PMA.

DOS PKI CAs must validate the requestor's authority to act in the name of the organization before issuing organizational certificates.

3.2.6 Criteria for Interoperation

The DOS PKI PMA must determine the criteria for cross certification with other Entities in accordance with Section 1.1.5 and the *Federal Public Key Infrastructure Bridge Application Process Overview* document, and the *Federal Public Key Infrastructure Annual Review Requirements* [AUDIT] document. Under no circumstances must any certificate have more than one intentional trust path to the FBCA.

Note: Multiple trust paths created as a result of certificate renewal or CA rekey do not violate the single trust path requirement above.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-Key

Re-keying a certificate means that the CMA creates a new certificate that has the same characteristics and level as the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key) and a different serial number and possibly different validity period.

If a DOS PKI AD Root CA re-key is required, a new cross-certificate must be requested from the FPKIPA. For any subordinate DOS PKI CA that requires a re-key, the DOS PKI AD Root CA will issue its new certificate.

Subscribers must periodically obtain new keys and re-establish identity as defined in Section 3.2. A DOS PKI CA may re-key Subscribers based on electronically authenticated Subscriber requests. Subscribers must stop using private keys before the public key expires. Decryption private keys do not have a lifetime so Subscribers may use these keys at any time to decrypt information.

PKI Sponsors for Role, Group, and Component certificates must also periodically obtain new keys and re-establish identity as defined in Section 3.2. A DOS PKI CA must re-validate the existence of the role or group; the PKI Sponsor's membership in the role or group; the authority of the PKI Sponsor to either hold or exercise the authority of the role or group; and the validity of the PKI Sponsor's personal certificates. For Component certificates, a DOS PKI CA must re-validate the identification and ownership of the component; the continued need for the certificate; the validity of any authorizations asserted in the certificate; and the validity of the requesting PKI Sponsor's authority to make the request and of his/her personal certificates.

Subscribers of DOS PKI CAs must identify themselves for the purpose of re-keying as required in the table below:

Table 3-3 Subscriber Routine Re-Key Identity Requirements

Assurance Level	Routine Re-key Identity Requirements for Subscriber Signature, Authentication and Encryption Certificates
Rudimentary	Identity may be established through use of current signature key.
Basic	Identity may be established through use of current signature key, except that identity must be reestablished through initial identity validation process at least once every 15 years from the time of initial registration.

Table 3-3 Subscriber Routine Re-Key Identity Requirements

Assurance Level	Routine Re-key Identity Requirements for Subscriber Signature, Authentication and Encryption Certificates
Medium (all policies)	Identity may be established through use of current signature key, except that identity must be established through initial identity validation process at least once every twelve (12) years from the time of initial registration. For certificates asserting policies mapped to id-fpki-certpcy-mediumDevice or id-fpki-certpcy-mediumDeviceHardware, identity may be established through the use of the device's current signature key or the signature key of the device's human sponsor.
High	Identity may be established through use of current signature key, except that identity must be established through initial identity validation process at least once every three years from the time of initial registration.

If DOS implements the capability of associating authorizations with a certificate, including any conveyed or implied by the subject's DN, the Subscriber and/or the Subscriber's organization must notify the appropriate CAs of the withdrawal of authorization. The CPS must document the mechanisms used to notify the appropriate CAs of this action. In such instances, withdrawal of authorization may result in revocation of the old certificate and, if necessary, the issuance of a new certificate with a different public key and the appropriate associated authorizations.

3.3.2 Identification and Authentication for Re-key after Revocation

For all levels of assurance, Subscribers requesting certificates after revocation, other than during a renewal or update action, must go through the initial identity authentication and registration requirements, as indicated in Section 3.2 to obtain a new certificate.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

The CMA must authenticate revocation requests in accordance with Section 4.9.3. The CMA may authenticate requests to revoke a certificate using signatures generated with that certificate's associated private key, regardless of whether or not the private key has been compromised.

3.5 IDENTIFICATION AND AUTHENTICATION FOR KEY RECOVERY REQUESTS

The DOS PKI supports key escrow and recovery of private decryption keys.

3.5.1 KRA Authentication

The KRA must authenticate to the KED directly or using a public key certificate issued by the associated DOS PKI. The assurance level of the certificate must be the same as or greater than

that of the certificate whose corresponding private key is being recovered and must meet the requirements of an RA credential.

3.5.2 KRO Authentication

The KRO must authenticate to the KRA using a public key certificate issued by the associated PKI. The assurance level of the certificate must be the same as or greater than that of the certificate whose corresponding private key is being recovered and must meet the requirements of an RA credential.

3.5.3 Subscriber Authentication

The Subscriber identity must be established as specified in Section 3.3.1 above. Alternatively, if the authentication cannot be verified using a public key certificate issued by the associated DOS PKI whose assurance level is the same as or greater than that of the certificate whose corresponding private key is being recovered, then the identity validation can use the steps outlined in Section 3.2.3.1.

For automated self-recovery, the Subscriber must be authenticated to the KED using a valid public key certificate. The assurance level of the Subscriber certificate must be equal to or greater than that of the certificate whose corresponding private key is being recovered.

3.5.4 Third-Party Requestor Authentication

The KRA or KRO must verify the identity and authorization of the Requestor prior to initiating the key recovery request.

Third-Party Requestor identity authentication must be commensurate with the assurance level of the certificate associated with the key being recovered. Identity must be established using one of the following methods:

- Procedures specified in Section 3.2.3 for authentication of an individual identity during initial registration for the specified certificate policy assurance level (an assurance level equal to or greater than the assurance level of the certificate whose corresponding private key is being recovered).
- Certificate-based authentication (e.g., digitally signed e-mail or client-authenticated TLS) that can be verified using current, valid (i.e., un-revoked) public key certificates at the requested certificate policy assurance level (an assurance level equal to or greater than the assurance level of the certificate whose corresponding private key is being recovered).

3.5.5 Data Decryption Server Authentication

The DOS PKI has not implemented a Data Decryption Server.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

The Certificate application process must provide sufficient information to:

- Establish the Applicant's authorization by the employing or sponsoring agency to obtain a certificate. See Section 3.2.3 for requirements.
- Establish and record the identity of the Applicant. See Section 3.2.3 for requirements.
- Obtain the Applicant's public key and verify the Applicant's possession of the private key. See Section 3.2.3 for requirements.
- Verify the information included in the certificate.

These steps may be performed in any order that does not defeat security, but all must be completed before certificate issuance.

This section specifies requirements for initial application for certificate issuance.

The DOS PKI AD Root CA may issue end-entity certificates to trusted DOS PKIPO personnel where necessary for the internal operations of the PKI AD Root CA. The DOS PKI AD Root CA does not issue end-entity certificates for any other reasons.

4.1.1 Who Can Submit a Certificate Application

For the DOS PKI AD Root CA, the DOS PKI PMA must submit the cross-certificate application to the FPKIPA.

For subordinate DOS PKI CAs, subordinate and/or supported activities must submit requests for subordinate PKI CA certificates to the Department of State DOS PKI MA using the contact information provided in Section 1.5.2.

Subscriber applicants must follow the procedures in Section 4.2 of this CP and the applicable CPS.

For Wildcard Certificates, the DOS PKIPO must develop, and the CMA must enforce policies and procedures for determining:

- Who can be a PKI Sponsor for a wildcard certificate and for managing the wildcard namespace
- Who can authorize a PKI Sponsor's control over the wildcard namespace.

For wildcard certificates, the DOS PKIPO must ensure that the Sponsor has documented mechanisms to manage and control the wildcard certificates and associated private keys.

4.1.2 Enrollment Process and Responsibilities

All communications supporting the certificate application and issuance process must be authenticated and protected from modification. Communications may be electronic or out-of-band.

Any electronic communication of shared secrets must be protected.

Where electronic communications are used, cryptographic mechanisms commensurate with the strength of the public/private key pair must be used.

Out-of-band communications must protect the confidentiality and integrity of the data.

Subscribers are responsible for providing accurate information on their certificate applications.

If databases or other sources are used to confirm Subscriber attributes, then these sources and associated information sent to a CA require:

- An auditable chain of custody be in place when information is obtained through one or more information sources
- All data received be protected and securely exchanged in a confidential and tamper evident manner and protected from unauthorized access.

Within the Department, only the DOS PKI AD Root CA may apply for cross certification with the FBCA and/or FCPCA, using the procedures outlined in the FBCA and/or FCPCA CP, the *Federal Public Key Infrastructure Bridge Application Process Overview* document, and the MOA.

Only the DOS PKI AD Root CA shall cross-certify with external CAs or establish subordinate CAs. A Certification Practices Statement, written to the format of the *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* [RFC 3647] must accompany all such requests. Entities applying for cross certification are responsible for providing accurate information on their certificate applications.

Upon issuance of a cross-certificate or a DOS PKI subordinate CA certificate, the DOS PKI CMA must manually check each certificate issued to the CA by the DOS PKI AD Root CA to ensure the proper population of each field and extension with the correct information before delivering the certificate to the External Entity CA or DOS PKI subordinate CA.

All CMAs must conform to the CPS as written for the applicable CA. All CMAs must authenticate, and protect from modification, communications among PKI authorities supporting the certificate application and issuance process.

4.2 CERTIFICATE APPLICATION PROCESSING

The CMA must verify the accuracy of information in certificate applications, using procedures specified in this CP and the applicable CPS, before the certificates are issued.

4.2.1 Performing Identification and Authentication Functions

For the DOS PKI AD Root CA, the DOS PKI OA must validate acceptance of applicant identification and authentication.

For subordinate DOS PKI CAs, the identification and authentication of the Subscriber must meet the requirements specified for Subscriber authentication as specified in Sections 3.2 and 3.3 of this CP. The applicant and the supporting CMA must perform the steps outlined in the applicable CPS when an applicant applies for a certificate. This CP identifies the components of the DOS PKI (e.g., CA or RA) that are responsible for authenticating the Subscriber's identity in each case.

CMAs must authenticate and protect from modification all communications supporting the certificate application and issuance process using mechanisms commensurate with the protection requirements of the data. CMAs must protect from unauthorized disclosure any electronic transmission of this data (i.e., encryption) commensurate with the protection requirements of the data.

4.2.2 Approval or Rejection of Certificate Applications

The DOS PKI PMA may require an initial compliance audit to ensure that the DOS PKI CAs and other Entity CAs are prepared to implement all aspects of their applicable CPS, before authorizing the DOS PKI OA to issue and manage certificates asserting Department of State certificate policies. DOS PKI CAs must only issue certificates asserting Department of State certificate policies and authorized Federal Common Policy OIDs upon receipt of written notification from the DOS PKI PMA authorizing them to do so.

The DOS PKI OA and RAs/LRAs may reject any Subscriber, group, role-based, or device certificate application that is incomplete, or that contains information that they cannot verify as accurate in accordance with Section 4.2.1. The CMA may afford Subscribers and Sponsors the opportunity to correct, complete and augment application information. Failure to do so will result in rejection of the application for the certificates. The CMA must submit a report via protected communications to the DOS PKI OA, outlining the circumstances for rejection and providing full identifying data about the applicant (i.e., the Subscriber or the Sponsor for group, role or device/application certificates).

For Device certificates, the CA must reject a certificate request if the requested Public Key has a known weak Private Key. Public key parameters generation and quality checking, must be conducted in accordance with Section 6.1.6 of this CP.

4.2.3 Time to Process Certificate Applications

CMAs must identify and authenticate Subscribers, organizations, components, and PKI Sponsors not more than 30 days prior to certificate issuance. Otherwise, the CMA must re-confirm the identity to ensure issuance of the certificates to the appropriate individual.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions During Certificate Issuance

It is the responsibility of the CMA to verify that the certificate information is correct and accurate. The CMA must check all CA certificates to ensure that all fields and extensions are properly populated.

Upon receiving the request, CMA must:

- Verify the identity of the requestor
- Verify the authority of the requestor and the integrity of the information in the certificate request
- Verify all attribute information received from a Subscriber before inclusion in a certificate
- Build and sign a certificate if all certificate requirements have been met (in the case of an RA, have the CA sign the certificate)
- Make the certificate available to the Subscriber after confirming that the Subscriber has formally acknowledged the obligations described in Section 9.6.3.

The CMA must not sign any certificate until the RA and/or LRA have completed all verifications and modifications, if any, to the CA's satisfaction, and the identification and authentication process set forth in the CP and appropriate CPS are complete. If an RA or LRA denies a certificate request, then the CA must not sign the requested certificate.

CMAs must verify all authorization and other attribute information received from an applicant. In most cases, the RA or LRA is responsible for verifying applicant data, but if CAs accept applicant data directly from applicants, then the CA is responsible for verifying the applicant data. The CMA must verify information regarding attributes via those offices or roles that have authority to assign the information or attribute. The applicable CPS shall describe these processes and relationships.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The DPS PKI MA must notify external entities of cross-certificate issuance, and the CMAs for DOS Subordinate CAs of subordinate CA certificate issuance.

Where notification is not an integral component of the issuance process (e.g., when individual is present as the certificate is generated on their token), DOS PKI CAs must proactively notify Subscribers and Sponsors that certificates have been generated.

4.4 CERTIFICATE ACCEPTANCE

For Rudimentary assurance, there is no stipulation.

For all other assurance levels, before a CA provides a Subscriber or Sponsor with the private key and allows its effective use:

- The CMA must convey the Subscriber's responsibilities to the Subscriber (and/or the Sponsor in the case of group, role-based and device certificates), as defined in Section 9.6.3
- The CMA must require and document the Subscriber's acceptance (and/or the Sponsor's acceptance in the case of group, role-based and device certificates) of those responsibilities

The CPS shall identify specific steps for conveying and documenting the acceptance of Subscriber and Sponsor responsibilities.

4.4.1 Conduct Constituting Certificate Acceptance

Failure to object to the certificate or its contents constitutes acceptance of the certificate.

4.4.2 Publication of the Certificate by the CA

As specified in 2.2.1, each DOS PKI CA must publish all CA and Subscriber certificates in certificate repositories accessible to Relying Parties.

FLAC certificates that contain the FASC-N or card UUID in the SAN extension, i.e., FLAC authentication certificates and FLAC card authentication certificates, must not be distributed via public repositories.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The DOS PKI PMA must notify the FPKIPA, and other entities cross-certified with the DOS PKI AD Root CA, at least two weeks prior to the issuance of a new DOS PKI CA certificate or upon issuance of an External Entity CA cross-certificate. In addition, all new artifacts (CA certificates, CRL DP, AIA and/or SIA URLs, etc.) produced because of the CA certificate issuance must be provided within 24 hours following issuance. The process for notifying the FPKIPA is included in the MOA.

The DOS PKI OA must notify DOS PKI CMAs responsible for all DOS PKI Subordinate CAs at least two weeks prior to the DOS PKI AD Root CA issuing a new DOS PKI CA certificate or a new External Entity CA cross-certificate. In addition, all new artifacts (CA certificates, CRL DP, AIA and/or SIA URLs, etc.) produced because of the CA certificate issuance must be provided within 24 hours following issuance.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

For Rudimentary assurance, this CP makes no stipulation.

For all other assurance levels, Subscribers must protect their private keys from access by other parties. Section 1.3 describes authorized and prohibited uses of PKI certificates.

DOS PKI CAs must specify restrictions in the intended scope of usage for a private key through certificate extensions, including the key usage and extended key usage extensions, in the associated certificate.

4.5.2 Relying Party Public Key and Certificate Usage

Certificates issued by DOS PKI CAs must specify restrictions on their use through critical certificate extensions, including the basic constraints and key usage extensions.

DOS PKI CAs must issue CRLs specifying the current status of all unexpired certificates.

Relying Parties should process certificate and certificate status information as specified in [X.509] when relying on DOS PKI certificates.

4.6 CERTIFICATE RENEWAL

Renewing a certificate means creating a new certificate with a new serial number where all certificate subject information, including the subject public key and subject key identifier, remain unchanged.

The new certificate may have an extended validity period and may include new issuer information (e.g., different CRL distribution point, AIA and/or be signed with a different issuer key).

Once renewed, the old certificate may or may not be revoked, but must not be used for requesting further renewals, re-keys, or modifications.

The DOS PKI does not perform certificate renewal.

4.6.1 Circumstance for Certificate Renewal

The DOS PKI does not perform certificate renewal.

4.6.2 Who may Request Renewal

The DOS PKI does not perform certificate renewal.

4.6.3 Processing Certificate Renewal Requests

The DOS PKI does not perform certificate renewal.

4.6.4 Notification of New Certificate Issuance to Subscriber

The DOS PKI does not perform certificate renewal.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

The DOS PKI does not perform certificate renewal.

4.6.6 Publication of the Renewal Certificate by the CA

The DOS PKI does not perform certificate renewal.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

The DOS PKI does not perform certificate renewal.

4.7 CERTIFICATE RE-KEY

Re-keying a certificate consists of creating a new certificate with new serial number and a different public key while retaining the remaining contents of the old certificate that describe the subject. The new certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key.

Once re-keyed, the old certificate may or may not be revoked, but must not be reused for requesting further renewals, re-keys, or modifications.

Subscribers of DOS PKI CAs must identify themselves for the purpose of re-keying as required in Section 3.3.1.

In the event that re-key of the DOS PKI AD Root CA is required, the DOS PKI PMA must notify the FPKIPA and request a new cross-certificate from the FPKIPA in accordance with this CP and the MOA. The DOS PKI PMA must also notify external entities cross-certified with the DOS PKI AD Root CA and arrange for the issuance of new cross-certificates in accordance with this CP and the applicable MOAs.

In the event that re-key of a DOS PKI Subordinate CA is required, the DOS PKI PMA must notify the FPKIPA in accordance with this CP and the MOA. The DOS PKI PMA must also notify external entities cross-certified with the DOS PKI AD Root CAs in accordance with this CP and the applicable MOAs. The Subordinate CA’s CMA must request authorization of the DOS PKI OA to receive a new Subordinate CA certificate from the DOS PKI AD Root CA.

4.7.1 Circumstance for Certificate Re-Key

Circumstances requiring certificate re-key include nearing the maximum usage period of a private key, certificate expiration, loss or compromise, issuance of a new hardware token, and hardware token failure.

Section 6.3.2 establishes maximum usage periods for private keys for both CAs and Subscribers.

4.7.2 Who May Request Certification of a New Public Key

The DOS PKI MA may request the re-key of the DOS PKI AD Root CA resulting in a new self-signed certificate for the new public key.

The DOS PKI PMA may request cross-certification of a new public key for a re-keyed DOS PKI AD Root CA by the FPKIPA under a currently valid MOA.

The DOS PKI PMA may request cross-certification of a new public key for a re-keyed DOS PKI AD Root CA by a currently cross-certified External Entity CA (other than the FPKI) under a currently valid MOA.

An official designated in the MOA for an External Entity CA currently cross-certified by the DOS PKI AD Root CA may request cross-certification of a new public key for the re-keyed External Entity CA.

The DOS PKI OA may request the re-key of a DOS PKI Subordinate CA resulting in a new subordinate CA certificate for the new public key issued by the DOS PKI AD Root CA.

For a Delegated OCSP Responder with a currently valid certificate, the DOS PKI OA may request re-key of the OCSP Responder's certificate by the issuing DOS PKI CA.

Subscribers who are the Subject of a currently valid certificate and PKI Sponsors of a currently valid certificate may request re-key of the certificate by the issuing CA. Additionally, a DOS Subordinate CA and its RAs may initiate re-key of a Subscriber's or Sponsor's certificate without a corresponding request.

4.7.3 Processing Certificate Re-keying Requests

Before performing re-key, the CMA must identify and authenticate the requestor by performing the identification processes defined in Section 3.2 or Section 3.3.

Digitally signed re-key requests must be validated before the re-key requests are processed.

The CMA must confirm the circumstances requiring re-key of end-entity certificates prior to issuing a new certificate and must ensure that the validity period of the re-keyed certificate meets the applicable requirements.

Before the DOS PKI AD Root CA issues a new cross-certificate, to a cross-certified External Entity CA that has been re-keyed, the CMA must verify that it is in accordance with:

- The current MOA between the DOS PKI and the external CA
- The external CA is currently in compliance with the MOA
- The validity period associated with the new cross-certificate does not extend beyond the period of the MOA
- Issuance is authorized by the DOS PKI PMA, and

- The request complies with the requirements of Section 4.7.2

4.7.4 Notification of New Certificate Issuance to Subscriber

The DOS Subordinate CAs proactively notify affected Subscribers of certificate re-key by any appropriate and secure means equivalent to the assurance level of the certificate issued (e.g., via an automated system notice, a digitally signed email (directly or via the LRA), secure telephone).

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

The Subscriber's or PKI Sponsor's failure to object to the certificate or its contents constitutes acceptance of the new certificate.

Subscribers and Sponsors with objections to the certificate must communicate in-person or by other secure verifiable means with the supporting RA/LRA. RAs/LRAs will allow sufficient time for the PKI Sponsor to review and respond, depending on the means and timeframe of delivery, but in no case more than seven calendar days.

4.7.6 Publication of the Re-keyed Certificate by the CA

As specified in Section 2.2.1 and 4.4.2, the DOS PKI CAs publish CA and Subscriber certificates in the appropriate certificate repositories.

4.7.7 Notification of Certificate Issuance by the CA to other Entities

If the DOS PKI AD Root CA issues a new self-signed certificate, two weeks prior to issuance the DOS PKI PMA must notify the FPKIPA and FPKIMA, other External Entity PKIs cross-certified with the DOS AD Root CA, and CMAs for DOS CAs subordinated to the DOS AD Root CA.

If a Subordinate DOS PKI CA is re-keyed, two weeks prior to issuance the DOS PKI OA must notify the DOS PKI PMA, the FPKIPA and FPKIMA, other External Entity PKIs cross-certified with the DOS AD Root CA, and CMAs for other DOS CAs subordinated to the DOS AD Root CA.

4.8 CERTIFICATE MODIFICATION

Modifying (or updating) a certificate means creating a new certificate that has the same or a different key and a different serial number, and that differs in one or more other fields from the old certificate.

Once modified, the old certificate may or may not be revoked, but must not be reused for requesting further renewals, re-keys, or modifications.

4.8.1 Circumstance for Certificate Modification

CA certificates and Delegated OCSP responder certificates whose characteristics have changed (e.g., assert new policy OID) may be modified. The new certificate may have the same or a different subject public key.

A certificate associated with a Subscriber whose characteristics have changed (e.g., name change due to marriage) may be modified. The new certificate must have a different subject public key.

The DOS PKI AD Root CA modifies the certificates it issued if a Trusted Role, Subordinate CA or cross-certified External Entity CA changes its name. The DOS PKI AD Root CA must not create a new certificate containing a public key that exists in another certificate.

DOS PKI Subordinate CAs modify the certificates they issued if the subject changes the name or other identifying data included in the certificate (e.g. assert new policy OID). The new certificate may have the same or a different subject public key.

4.8.2 Who May Request Certificate Modification

The DOS PKI MA may request the modification of the DOS PKI AD Root CA self-signed certificate.

The DOS PKI PMA may request modification of the current cross-certificate issued to the DOS PKI AD Root CA by the FPKIPA under a currently valid MOA for the following reasons:

- Modification of SIA extension; or
- Minor name changes (e.g., change CA1 to CA2) as part of key rollover procedures.

The DOS PKI PMA may request modification of the current cross-certificate issued to the DOS PKI AD Root CA by a currently cross-certified External Entity CA (other than the FPKI) under a currently valid MOA for the following reasons:

- Modification of SIA extension; or
- Minor name changes (e.g., change CA1 to CA2) as part of key rollover procedures.

An official designated in the MOA for an External Entity CA currently cross-certified by the DOS PKI AD Root CA may request cross-certification of a new public key for the re-keyed External Entity CA for the following reasons:

- Modification of SIA extension; or
- Minor name changes (e.g., change CA1 to CA2) as part of key rollover procedures.

The DOS PKI OA may request modification of the current certificate issued to a DOS PKI Subordinate CA by the DOS PKI AD Root CA for the following reasons:

- Modification of SIA extension; or
- Minor name changes (e.g., change CA1 to CA2) as part of key rollover procedures.

For a Delegated OCSP Responder with a currently valid certificate, the DOS PKI OA may request modification of the OCSP Responder's certificate by the issuing DOS PKI CA.

Subscribers who are the Subject of a currently valid certificate and PKI Sponsors of a currently valid certificate may request modification of the certificate. CAs and RAs may request certificate modification on behalf of a Subscriber.

4.8.3 Processing Certificate Modification Requests

Before performing certificate modification, the CMA must identify and authenticate the requestor by performing the identification processes defined in Section 3.2 or Section 3.3.

Proof of all subject information changes must be provided to the CMA and verified before the modified certificate is issued. If the modified certificate is issued with a new (different) public key, the additional requirements specified in Section 4.7.3 must also apply.

Digitally signed certificate modification requests must be validated before the requests are processed.

If an individual's authorizations or privileges change, such that the modified certificate indicates a reduction in privileges and authorizations, the old certificate must be revoked.

Before the DOS PKI AD Root CA issues a modified cross-certificate to a cross-certified External Entity CA, the CMA must verify that:

- The request is in accordance with the current MOA between the DOS PKI and the External Entity CA
- The External Entity CA is currently in compliance with the MOA
- The validity period associated with the modified cross-certificate does not extend beyond the period of the MOA
- Issuance is authorized by the DOS PKI PMA, and
- The request complies with the requirements of Section 4.8.2.

Except at Rudimentary assurance, if a Subscriber's common name is legally changed (e.g., due to marriage or divorce), then legal proof of the name change (i.e., the same requirements used to apply for a certificate) must be provided to the Designated Naming Authority to initiate the name change process in the directory structure. Once this change has taken place, the individual must appear before (or be validated by) an RA/LRA in order for an updated certificate having the new name to be issued.

4.8.4 Notification of New Certificate Issuance to Subscriber

The DOS Subordinate CAs proactively notify affected Subscribers of certificate modification by any appropriate and secure means equivalent to the assurance level of the certificate issued (e.g., via an automated system notice, a digitally signed email (directly or via the LRA), secure telephone).

4.8.5 Conduct Constituting Acceptance of Modified Certificate

The Subscriber's or PKI Sponsor's failure to object to the certificate or its contents constitutes acceptance of the new certificate.

Subscribers and Sponsors with objections to the certificate must communicate in-person or by other secure verifiable means with the supporting RA/LRA. RAs/LRAs will allow sufficient time for the PKI Sponsor to review and respond, depending on the means and timeframe of delivery, but in no case more than seven calendar days.

4.8.6 Publication of the Modified Certificate by the CA

As specified in Section 2.2.1 and 4.4.2, the DOS PKI CAs publish CA and Subscriber certificates in the appropriate certificate repositories.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Two weeks prior to the DOS PKI AD Root CA issuing a new self-signed certificate, the DOS PKI PMA must notify:

- The FPKIPA and FPKIMA
- Other External Entity PKIs cross-certified with the DOS AD Root CA, and
- The CMAs for DOS CAs subordinated to the DOS AD Root CA.

Two weeks prior to issuing a modified Subordinate DOS PKI CA certificate, the DOS PKI OA must notify:

- The DOS PKI PMA
- The FPKIPA and FPKIMA
- Other External Entity PKIs cross-certified with the DOS AD Root CA, and
- The CMAs for other DOS CAs subordinated to the DOS AD Root CA

4.9 CERTIFICATE REVOCATION AND SUSPENSION

For the DOS PKI AD Root CA, DOS Subordinate CAs, and cross-certified Entity CAs, certificates are revoked when the binding between the subject and the subject's public key defined within a certificate, excluding DN changes, is no longer considered valid. All revocation requests are authenticated as described in Section 5.7.

Revocation requests must be authenticated. PIV revocation requests are generally made in person since the request involves surrender or loss of the PIV Card; but written (email, cable, or memo) and telephonic requests may be accepted in the case of known or suspected key compromise, if call-back to a known individual and number (e.g., LRA or RSO) confirms the request. The RA or other Trusted Role may authenticate requests to revoke a certificate using that certificate's associated private key, regardless of whether or not the private key has been compromised.

For High, Medium Hardware, Medium, and Basic assurance, all CAs must publish CRLs as appropriate. OCSP responder certificates that include the *id-pkix-ocsp-nocheck* extension are not required to be listed in the CRLs when revoked.

The DOS PKI PMA must notify the FPKIPA and other entities cross-certified with the DOS PKI AD Root CA, at least two weeks prior to the revocation of a CA certificate, whenever possible. For emergency revocation of CA certificates, the notification procedures in Section 5.7 are followed.

4.9.1 Circumstances for Revocation

The CMA must revoke certificates issued by the DOS PKI AD Root CA under three circumstances:

- The first is when the DOS PKI PMA requests revocation of a DOS PKI AD Root CA-issued certificate. This will be the normal mechanism for revocation in cases where the DOS PKI PMA determines that a subordinate DOS PKI CA or a cross-certified Entity PKI does not meet the DOS PKI CP requirements or certification of the Entity PKI is no longer in the best interests of the Department of State or the Federal Government.
- The second is when the DOS PKI MA receives an authenticated request from a previously designated official of the cross-certified Entity responsible for the CA.
- The third is when the DOS PKIPO determines that an emergency has occurred that may affect the integrity of the certificates issued by a DOS PKI CA. Under such circumstances, the following individuals may authorize immediate certificate revocation:
  - DOS PKI PMA
  - DOS PKI MA

  The DOS PKI PMA must review the emergency revocation as soon as practicable.

The DOS PKI AD Root CA must, at a minimum, revoke certificates for the reason of key compromise upon receipt of an authenticated request from a subordinate DOS PKI CA or cross-certified Entity.

Whenever any of the three circumstances occur, the DOS PKI AD Root CA must revoke the associated certificate and place the revoked certificate on the appropriate revocation list. Revoked certificates must be included on all new publications of the certificate status information until the certificates expire.

The CMA must revoke the DOS PKI AD Root CA certificate, a subordinate DOS PKI CA's certificate, or an External Entity CA's cross-certificate, when the binding between the subject and the subject's public key defined within a certificate, excluding DN changes, is no longer considered valid.

The CMA must revoke a Subscriber certificate when the binding between the subject and the subject's public key defined within a certificate is no longer valid. Examples of circumstances that invalidate the binding are:

- Identifying information or affiliation components of any names in the certificate that become invalid.
- The Subscriber can be shown to have violated the stipulations of its Subscriber obligations and/or agreement
- The private key is suspected of compromise
- The user or other authorized party (as defined in the CPS) makes a formal request to the CMA asking to revoke his or her certificate
- Privileged attributes if implemented, asserted in the Subscriber's certificate are reduced
- The failure of a CA to adequately adhere to the requirements of this CP or the approved CPS. (e.g., there is strong evidence that the CA has failed to comply with the requirements of Section 6.7 of the CP
- Evidence that a wild card certificate has been issued with a name where the PKI Sponsor does not exercise control of the entire name space associated with the wildcard certificate.
- The CA is made aware that a wildcard certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name

Whenever any of the above circumstances are reported, the appropriate authority must review the circumstances and make a revocation decision. The revocation decision must be made based on appropriate criteria, to include:

- The nature of the alleged problem,
- The number of Certificate Problem Reports received about a particular Certificate or Subscriber, and
- Relevant legislation

If it is determined that revocation is required, the associated certificate must be revoked (similar to access revocation in 12 FAM 621.3-3) and placed on the CRL. Revoked certificates must be included on all new publications of the certificate status information, at least until the certificates expire.

4.9.2 Who Can Request Revocation

The DOS PKI PMA may direct revocation of a DOS PKI AD Root CA certificate, or certificate issued by the AD Root CA. Subordinate DOS PKI CAs and cross-certified Entity CAs must accept, at a minimum, revocation requests from Subscribers. The CMA may support requests for certificate revocation from other parties as specified in the appropriate CPS. A cross-certified Entity Principal CA may always revoke the certificate it has issued to a DOS PKI AD Root CA without DOS PKI PMA action.

Within the DOS PKI, a CA may summarily revoke certificates within its domain. An RA may request the revocation of a Subscriber's certificate on behalf of any authorized party as specified in its CPS or Subscriber agreements. A Subscriber can request the revocation of his or her own

certificate(s). The PKI Sponsor can request revocation of the device, group or role-based certificate for which he or she is responsible.

The DOS PKI must provide Subscribers, Relying Parties, Application Software Suppliers, and other third parties with instructions for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to certificates issued by the DOS PKI. These instructions must be posted on the following publicly available web site https://pkaps.pki.state.gov/pkiinfo/.

4.9.3 Procedure for Revocation Request

Upon receipt of a revocation request involving a DOS PKI AD Root CA-issued certificate, the DOS PKI MA must authenticate the request and apprise the DOS PKI PMA. The DOS PKI PMA may take whatever measures it deems appropriate to verify the need for revocation. If the revocation request appears valid, the DOS PKI PMA must direct the DOS PKI MA to revoke the certificate. The DOS PKI MA must give prompt oral or electronic notification to previously designated officials in all subordinate DOS PKI CAs and cross-certified external Entities having a Principal CA with which the DOS PKI AD Root CA interoperates. The DOS PKI PMA will notify the FPKIPA if a revocation is due to a certificate or system compromise, or a cross-certified Entity CA violation of their Memorandum of Agreement with the DOS PKI.

Subordinate DOS PKI CAs and cross-certified External Entity CAs must revoke certificates upon receipt of sufficient evidence of compromise or loss of the Subscriber’s corresponding private key.

A request to revoke a certificate must identify the certificate to be revoked; explain the reason for revocation; and provide a means for the request to be authenticated (e.g., digitally, or manually signed). Where Subscribers use hardware tokens, revocation is optional if all the following conditions are met:

- The revocation request was not for key compromise
- The cryptographic module does not permit the Subscriber to export the signature private key
- The Subscriber surrendered the token to the PKI CMA
- The token was zeroized or destroyed promptly upon surrender
- The token has been protected from malicious use between surrender and zeroization or destruction

In all other cases, revocation of the certificates is mandatory. Even where all the above conditions have been met, revocation of the associated certificates is recommended.

Upon receipt of a revocation request from the Subscriber or another authorized party, the CMA must authenticate the revocation request. At its discretion, the CA may take reasonable measures to verify the need for revocation. Revocation takes effect upon publication of status information.

For PKI implementations using hardware tokens, Subscribers leaving organizations that sponsored their participation in the PKI must surrender to their CMA (through any accountable mechanism) all cryptographic hardware tokens issued under the sponsoring organization before leaving the organization. If the CA cannot obtain the hardware tokens when a Subscriber leaves an organization, then the CA, immediately upon notification, must revoke all Subscribers' certificates associated with the un-retrieved tokens with key compromise specified as the reason. If later recovered, the token must be zeroized or destroyed promptly upon surrender and must be protected from malicious use between surrender and being zeroized or destroyed. If an organization terminates its relationship with the AD HACA such that it no longer provides affiliation information, the AD HACA must revoke all certificates affiliated with that organization.

If it is determined that a private key used to authorize the issuance of one or more certificates may have been compromised, all certificates directly or indirectly authorized by that private key since the date of actual or suspected compromise must be revoked or must be verified as appropriately issued.

4.9.4 Revocation Request Grace Period

The revocation request grace period is the time available to the Subscriber or PKI Sponsor within which they must make a revocation request after reasons for revocation have been identified.

There is no grace period for revocation under this policy; the Subscribers, PKI Sponsors and authorized parties must notify the CMA as soon as they identify the need to revoke a certificate. CAs will revoke certificates as quickly as practical upon receipt of a proper authenticated revocation request and must always revoke certificates within the time constraints described in Section 4.9.5. Also see Section 9.6.3.

4.9.5 Time Within Which CA Must Process the Revocation Request

The DOS PKI Root and subordinate CAs will revoke certificates as quickly as practical upon receipt of a proper authenticated revocation request. Revocation requests must be processed before the next CRL is published, excepting those requests validated within two hours of CRL issuance. Revocation requests validated within two hours of CRL issuance must be processed before the following CRL is published. A request is considered received when a trusted role authorized to revoke certificates, first accesses a valid request.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying parties are expected to verify the validity of certificates as specified in [RFC 5280].

Use of revoked certificates could have damaging or catastrophic consequences. The Relying Party and/or System Accreditor make any determinations on the matter of how often new revocation data should be obtained, considering the risk, responsibility, and consequences for using a certificate whose revocation status cannot be guaranteed.

4.9.7 CRL Issuance Frequency

The DOS PKI AD Root CA and all subordinate DOS PKI CAs must issue CRLs as appropriate. For this CP, issuance encompasses both CRL generation and publication. To the extent practical, the CMA must check the contents of CRLs before issuance to ensure that all information is correct.

To ensure timeliness of information, every CA must periodically issue and post a CRL to a repository, even if there are no changes or updates required. A CA may issue CRLs more frequently than required. DOS PKI CAs must always post an early update to an applicable Revocation List in the event of a revocation due to key compromise. CRL validity periods will typically be longer than the next update, to facilitate caching for offline or remote (e.g., laptop) operation and other purposes. The CA must automatically overwrite the previously posted CRL in the repository by the posting of the new CRL.

For each assurance level, the minimum issuance frequencies for routine CRLs are as follows:

Table 4-1 CRL Issuance Frequency

Assurance Level	Maximum Interval for Routine CRL Issuance	
	Online	Offline*
Rudimentary	No Stipulation	No Stipulation
Basic	18 hours	35 Days
Medium (all policies)	18 hours	35 Days
High	18 hours	35 Days

*An offline CA may incorporate locally attached network equipment such as an HSM or storage array. The CA system and any such locally attached network equipment must be completely isolated (air-gapped) from all other networks and computing systems.

For the DOS PKI AD Root CA, the interval between CRLs must not exceed 18 hours. In the case of revocation of a subordinate CA certificate, the appropriate DOS PKI AD Root CA must issue an emergency CRL within six hours of notification. Subordinate CAs that issue certificates to subscribers or operate on-line, must issue CRLs at least once every 18 hours, and the *nextUpdate* time in the CRL may be no later than 180 hours after issuance time (i.e., the *thisUpdate* time).

CAs may be operated in an offline manner if the CA only issues:

- CA certificates
- (optionally) CSS certificates
- (optionally) end user certificates solely for the administration of the CA, and

- (optionally) end user certificates that contain the contentSigning EKU.

For an offline CA, the interval between routine CRL issuance must not exceed 35 days. An offline CA must publish CRL within six hours of notification of compromise or any other reason that may require certificate revocation of a related or cross-certified CA and/or OCSP responder. An offline CA need not publish a CRL if there are no end-entity Subscribers to that CA. CAs must publish certificate status information not later than the next scheduled update.

4.9.8 Maximum Latency for CRLs

CRLs must be published within 4 hours of generation.

For DOS PKI CAs that operate offline, pre-generated CRLs intended for publication more than 4 hours after generation must be protected in the same manner as the CA. All pre-generated CRLs not yet published must be securely destroyed whenever the CA revokes any certificate. The CPS must describe protections and processes used to generate and protect of any pre-generated CRLs.

Furthermore, each CRL must be published no later than the time specified in the nextUpdate field of the previously issued CRL for same scope.

Note: If CRLs are pre-generated, the thisUpdate field will be the date of generation. The nextUpdate value will be beyond the date of planned publication.

4.9.9 On-line Revocation or Status Checking Availability

Under this CP the DOS PKI CAs and Relying Party client applications may optionally support online status checking. Since the Department of State operates in some environments that cannot accommodate online communications, all DOS PKI CAs must be required to support CRLs.

Note: The FCPF CP requires that on-line status checking via OCSP [RFC 2560] must be supported for PIV certificates issued by the DOS PIV CA2 and the derived PIV certificates issued by the DOS DPC CA.

The FBCA CP requires that on-line status checking via OCSP [RFC 2560] must be supported for publicly trusted server authentication and code signing certificates. The DOS PKI does not issue publicly trusted server authentication or code signing certificates.

Online certificate status services used to verify certificates asserting Department of State certificate policies must perform the following actions:

- Certificates indicated as being valid have a chain of valid certificates (valid as defined by X.509) linking back to the appropriate DOS PKI AD Root CA
- Each certificate in the certificate chain used to validate the certificate whose status is being requested is checked for revocation, such that the Relying Party need not check more than one CSA to validate a Subscriber certificate
- The certificate status response makes clear which attributes, other than certificate subject name the CSA authenticates

If a DOS PKI CA supports on-line revocation/status checking, the latency of certificate status information distributed on-line by CAs, or their delegated status responders must meet or exceed the requirements for CRL issuance stated in Section 4.9.7.

Where on-line status checking is supported, status information must be updated and available to relying parties within 18 hours of certificate revocation.

For the status of Subscriber Certificates:

> The CA must update information provided via an Online Certificate Status Protocol at least every 18 hours. OCSP responses from this service must have a maximum expiration time of ten days.

For the status of Subordinate CA Certificates:

> The CA must update information provided via an Online Certificate Status Protocol whenever CRLs are generated and at least within 18 hours after revoking a Subordinate CA Certificate.

The CA must operate and maintain its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

The CA must maintain an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by the CA.

The CA must maintain a continuous 24x7 ability to respond internally to a high-priority certificate problem report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

4.9.10 On-line Revocation Checking Requirements

On-line revocation status checking is optional for relying parties. For certificates where revocation status online checking is not available, CRLs must be used.

Clients using online revocation checking need not obtain or process CRLs, at their own discretion.

4.9.11 Other Forms of Revocation Advertisements Available

A DOS PKI CA may use other methods to publicize the certificates it has revoked. Any alternative method must meet the following requirements:

- The alternative method must be described in the CA’s appropriate CPS.
- The alternative method must provide authentication and integrity services commensurate with the assurance level of the certificate being verified.
- Any alternate forms used to disseminate revocation information must be implemented in a manner consistent with the security and latency requirements for the implementation of CRLs and online revocation and status checking in Sections 4.9.5, 4.9.7, 4.9.8, and 4.9.9.

4.9.12 Special Requirements Related To Key Compromise

In the event of a DOS PKI AD Root CA or cross-certified Entity Principal CA private key compromise or loss, the cross-certificates must be revoked and an emergency CRL must be published as soon as feasible, and all cross-certified entities notified.

For subordinate DOS PKI CAs, when a CA certificate is revoked or Subscriber certificate is revoked because of compromise, or suspected compromise, of a private key, an emergency CRL must be issued and published as specified below:

Table 4-2 Emergency CRL Issuance Frequency

Assurance Level	Maximum Latency for Emergency CRL Issuance
Rudimentary	No stipulation
Basic	18 hours after notification
Medium (all policies)	18 hours after notification
High	6 hours after notification

The CRL must contain codes identifying the reason for revoking a certificate and/or specific key pair.

4.9.13 Circumstances for Suspension

The DOS PKI AD Root CA shall not suspend certificates.

DOS PKI Subordinate CAs may support certificate suspension and restoration for Subscriber certificates. If suspension and restoration are supported, the DOS PKI CPS must describe under what circumstances certificates may be suspended and restored and provide details for the corresponding sections below.

For DOS CAs that support suspension, those authorized to request suspension of a certificate must be identified.

4.9.14 Who can Request Suspension

The DOS PKI AD Root CA does not support suspension of certificates it issues.

For DOS PKI Subordinate CAs, an RA may request the suspension of a Subscriber's certificate on behalf of any authorized party as specified in the DoS PKI CPS or Subscriber agreements. The PKI Sponsor can request suspension of the device, group or role-based certificate for which he or she is responsible.

4.9.15 Procedure for Suspension Request

The request to suspend a certificate must include:

- Authentication of the Requestor,
- Identification of the certificate to be suspended, and
- Explanation of the reason for suspension

The DOS AD Root CA does not support suspension of certificates it issues.

DOS Subordinate CAs shall suspend certificates upon receipt of an authenticated request that meets the requirements stipulated in this CP and the DoS PKI CPS. A request to suspend a certificate must identify the certificate to be suspended and provide a means for the request to be authenticated (e.g., digitally signed).

Upon receipt of a certificate suspension request, the CA must authenticate the request. Suspension takes effect upon publication of status information.

For DOS PKI CAs that support suspension, all suspended certificate serial numbers must be populated on a full CRL within a timeframe specified in Section 4.9.7. The reason code CRL entry extension shall be populated with "certificateHold".

4.9.16 Limits on Suspension Period

The maximum period of time that a certificate may be suspended must be specified. The CPS must describe in detail how this maximum suspension period is enforced. If the Subscriber has not removed the certificate from hold (suspension) within that period, the certificate must be revoked. Certificates must not be published on a CRL with a reason code of "certificateHold" beyond the expiration date of the certificate.

To mitigate the threat of an unauthorized person removing the certificate from hold, the identity of the RA or authorized individual removing the suspension should be authenticated using a mechanism equivalent or higher than the assurance level of the certificate being unsuspended.

4.10 CERTIFICATE STATUS SERVICES

CSSs are not a required component of the DOS PKI under this CP. If supported, the CSS is considered an integral part of the CA system.

4.10.1 Operational Characteristics

A CSS must meet the following requirements:

- The CSS must be operated in compliance with this CP
- Information exchanged between the CA and the CSS must be authenticated and protected from modification using mechanisms commensurate with the requirements of the data to be protected by the certificates being issued

- Accurate and up-to-date information from the associated CA must be used to provide the revocation status
- Revocation status responses must provide authentication and integrity services commensurate with the requirements of the data to be protected by the certificates being issued, to include the status of the certificate and the time the status indication was generated
- Latency of certificate status information must meet or exceed the requirements for CRL issuance stated in Section 4.9.7

4.10.2 Service Availability

Where applicable this must be described in the CPS.

4.10.3 Optional Features

Where applicable this must be described in the CPS.

4.11 END OF SUBSCRIPTION

This CP makes no stipulation.

4.12 KEY ESCROW AND RECOVERY

The DOS PKI AD Root CA must not perform any encryption key recovery functions involving subordinate DOS PKI CAs or cross-certified Entity CAs. The DOS PKI AD Root CA must not store any information encrypted by subordinate DOS PKI CA's public keys that may require key recovery capabilities. However, when encryption key pairs need to be issued by the DOS PKI AD Root CA to cover repository system access or for other purposes, the DOS PKI PMA must publish applicable requirements for that purpose.

4.12.1 Key Escrow and Recovery Policy and Practices

DOS PKI CA private keys are never escrowed.

Under no circumstances will a Subscriber's signature key be escrowed, or any third party hold in trust a Subscriber's private signature key.

Under this CP Subscriber key management keys may be escrowed to provide key recovery.

Note: The FCPF CP requires that the PIV human Subscriber key management keys issued by the DOS PIV CA2 must be escrowed to provide key recovery. These escrowed keys must be maintained within an online KED for a minimum of one year after the expiration of the associated public key certificate.

DOS PKI Key Recovery Policy is documented in this CP, and DOS PKI Key Recovery practices are documented in the DOS PKI CPS. The practices must satisfy privacy and security requirements for the CAs issuing and managing digital certificates under this DOS PKI CP.

Subordinate DOS PKI CAs may escrow Subscriber key management keys to provide for recovery of those keys. The CA must protect escrowed keys at no less than the level of security in which they are generated, delivered, and protected by the Subscriber.

4.12.1.1 Key Escrow Process and Responsibilities

Human subscriber private keys (i.e., decryption private keys) associated with a key management certificate must be securely escrowed by the KED. The DOS PKI CA must ensure that the keys are escrowed successfully prior to issuing the key management certificates.

Subscriber private keys must be protected during transit and storage using cryptography at least as strong as the key being escrowed.

Subscribers must be notified that the private keys associated with their encryption certificates will be escrowed.

4.12.1.2 Key Recovery Process and Responsibilities

Communications between the various key recovery participants (KED, DDS, KRA, KRO, Requestor, and Subscriber) must be secured from protocol threats such as disclosure, modification, replay, and substitution. The strength of all cryptographic protocols must be equal to or greater than that of the keys they protect.

During delivery, escrowed keys must be protected against disclosure to any party except the Requestor.

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

Subscribers may use electronic or manual means to request their own escrowed keys from the key recovery service. The Subscriber may submit the request to the KRA or KRO. If the request is made electronically, the subscriber must digitally sign the request or authenticate to a recovery service using an associated authentication or signature certificate with an assurance level equal to or greater than that of the escrowed key. Manual requests must be made in person and include proper identity verification by the KRA in accordance with Section 3.2.3.1.

Third-Party Requestors may use electronic or manual means to request a Subscriber's escrowed keys. The Requestor must submit the request to the KRA or KRO. If the request is made electronically, the Requestor must digitally sign the request using an authentication or signature certificate, trusted by the DOS, with an assurance level equal to or greater than that of the escrowed key. Manual requests must include proper identity verification by the KRA in accordance with Section 3.2.3.1.

Third Party key recovery in and of itself does not require revocation of a Subscriber certificate. This does not prohibit Subscribers from requesting revocation of their own certificates for any reason.

4.12.1.2.1 *Key Recovery Through KRA*

The KRA must provide access to a copy of an escrowed key only in response to a properly authenticated and authorized key recovery request. Such access requires the actions of at least two KRAs. All copies of escrowed keys must be protected using two-person control procedures during recovery and delivery to the authenticated and authorized Requestor. Split key or password procedures are considered adequate two-person controls, provided they comply with technical controls in Section 6.2.2.

A combination of physical, procedural, and technical security controls can be used to enforce continuous two-person control during recovery and delivery of escrowed keys. The KRS should be designed to maximize the ability to enforce two-person control technically.

The KRA is not required to notify subscribers of a third-party key recovery.

4.12.1.2.2 *Automated Self-Recovery*

A current Subscriber's escrowed keys may be provided directly to the Subscriber without imposition of two-person control requirements. The KED must only provide escrowed keys to current Subscribers without two-person control upon:

- Verifying that the authenticated identity of the Requestor is the same as the Subscriber associated with the escrowed keys being requested

- Sending notification to the Subscriber of all attempts (successful or unsuccessful) to recover the Subscriber's escrowed keys that are made by entities claiming to be the Subscriber. If the KED does not have information (e.g., an e-mail address) necessary to send notification to the Subscriber of a key recovery request, then the KED must not provide the Subscriber with the requested key material using the automated recovery process. Where possible, the e-mail address will be from the subject alternative name field of the certificate being recovered.

- Ensuring that the escrowed keys are being sent only to the authenticated Subscriber associated with the escrowed keys

- Ensuring that the escrowed keys are encrypted during transmission using cryptography of equal or greater strength than provided by the escrowed keys.

4.12.1.2.3 *Key Recovery During Token Issuance*

When a Subscriber (individual and/or group/role sponsor or member) is issued a new certificate on a hardware token, private key management keys for the Subscriber may be recovered as part of the issuance process as long as the KED uses secure means, such as Global Platform Secure Channel Protocol, to inject the key history onto the hardware token directly.

The hardware token must meet FIPS 140 Level 2 hardware requirements, and the key must be injected into the token such that it is not thereafter exportable.

4.12.1.2.4 *Key Recovery by Data Decryption Server*

The DOS PKI has not implemented a Data Decryption Server.

4.12.1.3 Who Can Submit a Key Recovery Application

Subscribers may request recovery of their own escrowed keys.

Key recovery may be requested by an internal Third-Party Requestor in accordance with the key recovery practices specified in the DOS PKI CPS.

Key recovery may also be requested and by authorized external Third-Party Requestors (e.g., law enforcement personnel with a court order from a competent court) in accordance with the key recovery practices specified in the DOS PKI CPS.

4.12.1.3.1 *Requestor Authorization Validation*

The KRA or the KRO, as an intermediary for the KRA, must validate the authorization of the Requestor in accordance with the key recovery practices specified in the DOS PKI CPS.

The DOS PKI CPS must specify internal notification requirements for External Third-Party key recovery requests and account for situations where the law requires the KED to release the Subscriber's private key without organizational notification.

Nothing in this document is intended to change the current procedures for obtaining information about individuals in connection with such requests.

4.12.1.3.2 *Subscriber Authorization Validation*

Current Subscribers are authorized to recover their own escrowed key material.

4.12.1.3.3 *KRA Authorization Validation*

The KED must verify that the KRA has appropriate privileges to obtain the keys for the identified Subscriber's organization.

4.12.1.3.4 *KRO Authorization Validation*

The KED or KRA must verify that the KRO is authorized to request keys for the identified Subscriber.

4.12.1.3.5 *Data Decryption Server Authorization Validation*

The DOS PKI has not implemented a Data Decryption Server.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

The DOS PKI does not support session key encapsulation and recovery.

5. FACILITY MANAGEMENT AND OPERATIONS CONTROLS

5.1 PHYSICAL CONTROLS

All DOS PKI CA equipment, including CA cryptographic modules, must be protected from unauthorized access at all times. The CA must implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. CA cryptographic tokens must be protected against theft, loss, and unauthorized use.

All the physical control requirements apply equally to all DOS PKI CAs, and any remote workstations used to administer the CAs except where specifically noted.[14]

5.1.1 Site Location and Construction

The location and construction of the facility housing DOS PKI CA equipment, as well as sites housing remote workstations used to administer the CAs, must be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards, high security locks and intrusion sensors, must provide robust protection against unauthorized access to CA equipment and records.

The location and construction of any facility housing CMA equipment and operations must be in accordance with the Department of State Foreign Affairs Manual, Chapter 12, Section 620 (12 FAM 620), *Unclassified Information System Security Policies*.

5.1.2 Physical Access

5.1.2.1 Physical Access for CA Equipment and Remote CA Administration Workstations

5.1.2.1.1 *Physical Access for CA Equipment*

The CMA staff and DOS PKI facilities must protect DOS PKI CA equipment from unauthorized access at all times. The security mechanisms must be commensurate with the level of threat in the equipment environment. Since the DOS PKI AD Root CA and subordinate CAs must plan to issue certificates at all levels of assurance, the DOS PKI OA must operate and control all CAs on the presumption that each must issue at least one High Assurance certificate.

The physical security requirements pertaining to DOS PKI CAs that issue only Basic Assurance certificates are:

- Ensure no unauthorized access to the hardware is permitted

[14] The phrase "remote workstations used to administer the CAs," refers to a system used to access either the system hosting the CA or the CA itself through external networks for maintenance and administration. See Section 6.6.1 for additional technical controls required of remote workstations. This term does not refer to consoles within the CA's security perimeter or to Registration Authority workstations.

- Ensure all removable media and paper containing sensitive plain-text information is stored in secure containers.

In addition to those requirements, the following requirements must apply to DOS PKI CAs that issue Medium, Medium Hardware, or High assurance certificates:

- Ensure manual or electronic monitoring for unauthorized intrusion at all times
- Ensure an access log is maintained and inspected periodically
- Require two-person physical access control to both the cryptographic module and computer system.

Multi-person physical access control to CA equipment can be achieved by any combination of two or more trusted roles (see Section 5.2.2) as long as the tasks being conducted are segregated in accordance with the requirements and duties defined for each trusted role.

The CMAs must inactivate removable CA cryptographic modules before storage. Removable cryptographic modules, removable media, activation information used to access or enable cryptographic modules or other sensitive CMA equipment, and paper or other media containing sensitive plain-text information, must be placed in secure locked containers when not in use. Such containers must be sufficient for housing equipment and information commensurate with the classification, sensitivity, or value of the information protected by the certificates issued by the CA.

Activation data must be either memorized, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and must not be stored with the cryptographic module or removable hardware associated with remote workstations used to administer the CA.

A security check of the facility housing DOS PKI CA equipment or remote workstations used to administer the CAs (operating at the Basic Assurance level or higher) must occur before leaving the facility unattended. At a minimum, the check must verify the following using the DOS Standard Form 701:

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

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

For CAs operating at the Medium, Medium Hardware, or High assurance level the following requirements must also apply:

- CA equipment is manually or electronically monitored for unauthorized intrusion at all times
- A visitor access log is maintained and periodically inspected.

5.1.2.1.2 *Physical Access for Remote CA Administration Workstations*

Remote CA administration workstations that authenticate directly to the CA using hardware certificates issued at a level of assurance commensurate with that of the CA and communicate via secured protocols are not subject to the physical access controls of the CA but must be protected from unauthorized access while the cryptographic module is installed and activated. Remote CA administration workstations must implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. These security mechanisms must be commensurate with the level of threat in the workstation environment.

- CMAs must only install Security Management Administration (SMA) software on workstations specifically designated for remote CA administration
- Remote CA administration workstations must be equipped with removable hard drives, and these hard drives must be protected against theft, loss, and unauthorized use.
- When not in use, the CMAs must place removable hard drives, CMA cryptographic modules, removable media, and any activation information used to access or enable CMA cryptographic modules or CMA equipment, or paper containing sensitive plain-text information, in locked containers. Such containers must be sufficient for housing equipment and information commensurate with the classification, sensitivity, or value of the information protected by the certificates issued by the CMA.
- CMAs must implement physical access controls on remote CA administration workstations as appropriate to reduce the risk of equipment tampering even when the cryptographic module and hard drive are not installed and activated
- CMA cryptographic tokens must be protected against theft, loss, and unauthorized use
- Implement access controls and communication mechanisms on all remote CA administration workstations to include identification of both the CMA staff and workstation identification by the firewall and/or CA

5.1.2.2 Physical Access for RA Equipment

RA equipment must be protected from unauthorized access while the RA's cryptographic module is installed and activated. RAs must implement physical access controls on RA equipment as appropriate to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. RA cryptographic tokens must be protected against theft, loss, and unauthorized use. These security mechanisms must be commensurate with the level of threat in the RA equipment environment.

5.1.2.3 Physical Access for CSS Equipment

Physical access control requirements for CSS equipment that has signing capability must meet the CA physical access requirements specified in Section 5.1.2.1.1. CSS equipment that does not have a private signing key and only distribute pre-generated OCSP responses are not required to meet these requirements.

5.1.2.4 Physical Access for CMS Equipment

Physical access control requirements for CMS equipment must meet the DOS PKI CA physical access requirements specified in Section 5.1.2.1.1.

5.1.2.5 Physical Access for KED Equipment

Physical access control requirements for KED equipment that store private keys must meet the CA physical access requirements specified in Section 5.1.2.1.1.

5.1.2.6 Physical Access for DDS Equipment

The DOS PKI has not implemented a Data Decryption Server.

5.1.2.7 Physical Access for KRA and KRO Equipment

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

5.1.3 Power and Air Conditioning

The facility housing CA equipment must have power and air conditioning sufficient to create a reliable operating environment. DOS PKI CAs operating at a Basic, Medium, or High assurance level must have backup capability sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. In addition, the DOS PKI CA directories (containing CA certificates and CRLs) must have uninterrupted power sufficient for a minimum of six (6) hours operation in the absence of commercial power, to maintain availability and avoid denial of service.

5.1.4 Water Exposures

CA equipment must be installed such that it is not in danger of exposure to water and ensure installation of moisture detectors in areas susceptible to flooding. This requirement excludes potential water damage from fire prevention and protection measures (e.g., sprinkler systems). Contingency plans for a CA that has sprinklers for fire control must address recovery if the sprinklers malfunction, or cause water damage outside the fire area. This policy makes no stipulation on prevention of exposure of CA equipment to water beyond that called for by 12 FAM 629.4-2 and standard practices for DOS Data Centers.

5.1.5 Fire Prevention and Protection

This policy makes no stipulation on fire prevention and protection of CA equipment beyond that called for by 12 FAM 629.4-4 and standard practices for DOS Data Centers. A description of the CMA's approach for recovery from a fire disaster must be included in the Disaster Recovery Plan required by Section 5.7.

5.1.6 Media Storage

Sensitive CA media must be stored to protect it from accidental damage (water, fire, electromagnetic) and unauthorized physical access. Media that contains security audit, archive or backup information must be stored in a location separate from the CA equipment.

5.1.7 Waste Disposal

Normal office waste must be removed or destroyed in accordance with local policy. Sensitive media and documentation that are no longer needed for operations must be destroyed before disposal, such that the information is unrecoverable.

5.1.8 Off-Site backup

DOS PKI CAs operating at Basic, Medium, Medium Hardware, or High assurance levels must make system backups sufficient to recover from system failure, on a periodic schedule specified in the CPS. The DOS CMAs must perform and store full backups of all DOS PKI CAs off-site from the CA equipment not less than once per week.

The CMAs must retain not less than the latest full backup. The backup(s) must be stored at a site with physical and procedural controls commensurate to that of the operational CA system.

For offline CAs, the backup must be performed each time the system is turned on or once per week, whichever is less frequent.

Requirements for CA private key backup are specified in Section 6.2.4.

5.2 PROCEDURAL CONTROLS

Unless stated otherwise, the requirements in this section apply equally to all DOS PKI CAs.

5.2.1 Trusted Roles

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

An auditable record must be created identifying when personnel are added or removed from a trusted role, as well as who added or removed them from the role. The individual who authorized the role assignment, or any series of role assignments over a given period of time, must also be traceable via audit and archive records.

5.2.1.1 Certification Authority Trusted Roles

The requirements of this policy are defined in terms of the following four roles. Additional roles may be defined in the applicable CPS provided the following separation of duties are enforced.

- *Administrator* – authorized to install, configure, and maintain the CA and KED; establish and maintain system accounts; configure audit parameters; and generate PKI component keys
- *Officer* – authorized to request or approve certificate issuance and revocations
- *Auditor* – authorized to review, maintain, and archive audit logs
- *Operator* – authorized to perform system backup and recovery and other routine operations in support of the CA and KED equipment

Administrators do not issue certificates to Subscribers.

These four roles are employed at the CA, CMS, KRS, and CSS locations as appropriate. Separation of duties must comply with Section 5.2.4, and requirements for two-person control with Section 5.2.2, regardless of the titles and numbers of Trusted Roles.[15]

The following subsections provide a more detailed description of the responsibilities for each of these roles:

5.2.1.1.1 ***Administrator***

The Administrator role is responsible for the following:

- Installation, configuration, and maintenance of the CA and KED equipment to include the operating system (OS)
- Establishing and maintaining CA and KED system accounts
- Configuring certificate profiles or templates and audit parameters
- Generating and backing up CA and KED keys

Administrators do not issue certificates to Subscribers.

See Section 5.2.4 for role separation requirements.

5.2.1.1.2 ***Officer***

[15] A person providing trusted role support for one CA may fill the same or different trusted role position for another CA, so long as the provisions of Section 5.2 of this CP and the applicable CPS are met for each individual CA.

The Officer role is responsible for issuing certificates[16], that is:

- Registering new Subscribers and securely requesting the issuance of certificates
- Verifying the identity of Subscribers, validity of documentation, and accuracy of information included in certificates
- Approving and executing the issuance or recovery of certificates
- Requesting, approving, and executing the revocation of certificates
- Receiving, controlling, and distributing Subscriber certificates on FIPS 140 Level 2 compliant hardware tokens (cryptographic modules containing the Subscriber's private key), as specified in this CP and the applicable DOS CPS

The Officer also performs the administration and operation of the RA workstation.

See Section 5.2.4 for role separation requirements.

5.2.1.1.3 *Auditor*

The Auditor role is responsible for the following:

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

See Section 5.2.4 for role separation requirements.

5.2.1.1.4 *Operator*

The Operator role is responsible for the routine operation of the CA and KED equipment and operations such as system backups and recovery, changing recording media, the access control to and transport of sensitive material under multi-person control, and other support of PKI ancillary components and functions. The Operator typically provides PKI system support for those functions not assigned to the Administrators or Officers.

An Administrator or Officer may also function as an Operator, but in doing so shall not be both an Administrator and an Officer, as described in Section 5.2.4, or have the permissions for both roles. The Operator role itself must have no administrator/super user/root access to the operating system, or certificate management permissions on the CA application, or key recovery permissions on the KED application, but may have "read-only" permissions to support routine operations. An Operator may have these permissions as part of the Administrator or Officer roles but must meet role separation requirements in Section 5.2.4.

[16] The Officer (a.k.a. Security Officer, Registration Authority) may not register, request, or approve issuance or recovery of their own certificates; or, verify identity, validity of documentation, or accuracy of information pertaining to their own identity.

5.2.1.2 Registration Authority Trusted Roles

An RA may be considered an Officer as defined in Section 5.2.1.1 and is responsible for:

- verifying initial identity, as described in Section 3.2
- entering Subscriber information, and verifying correctness
- securely communicating requests to and responses from the CA
- receiving and distributing Subscriber certificates.

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

5.2.1.3 Key Recovery Trusted Roles

Due to the security implications and impacts to confidentiality services associated with key recovery, the number and location of Key Recovery Trusted Roles should be closely controlled.

The DOS PKI will use a limited number of RAs to fulfill the Key Recovery functions.

5.2.1.3.1 *Key Recovery Agent (KRA)*

A limited number of DOS PKI RAs shall be appointed as RA/KRAs.

The RA/KRAs is responsible for the following:

- Authorized to verify a Requestor's identity and authorization as stated by this policy
- Authorized to build key recovery requests on behalf of authorized Requestor
- Authenticating requests and recovering copies of escrowed keys
- Distributing copies of recovered keys to the Requestor, with protection as described in Section 4.12.1.2.1.

5.2.1.3.2 *Key Recovery Official (KRO)*

A KRO's responsibilities are to ensure that the following functions occur according to the stipulations of the applicable policy:

- Authorized to verify a Requestor's identity and authorization as stated by this policy,
- Authorized to build key recovery requests on behalf of authorized Requestor,
- Authorized to securely communicate key recovery requests to and responses from the KRA, and
- Authorized to participate in distribution of escrowed keys to the Requestor, as specified in the associated CPS.

5.2.2 Number of Persons Required per Task

Only one person is required per task for CAs operating at the Rudimentary and Basic Levels of Assurance.

Medium, Medium Hardware, and High assurance CAs must enforce multi-person controls on the CA private signing key and KED key to prevent duplication or theft without collusion.

Two or more persons are required for DOS PKI CAs operating at the Medium, Medium Hardware, or High Levels of Assurance for the following tasks:

- CA or KED key generation
- CA signing key activation
- CA or KED private key backup

Medium, Medium Hardware, and High assurance CAs must enforce multi-person controls on the CA private signing key and KED key to prevent duplication or theft without collusion.

Where multiparty control is required, at least one of the participants must be an Administrator. All participants must serve in a trusted role as defined in Section 5.2.1. Multiparty control for logical access must not be achieved using personnel that serve in the Auditor Trusted Role. The participation of two KRAs is required for third-party key recovery.

5.2.3 Identification and Authentication for Each Role

At all assurance levels other than Rudimentary, an individual must identify and authenticate him or herself before being permitted to perform any actions set forth above for that role or identity.

5.2.4 Roles Requiring Separation of Duties

Requirements for the separation of roles, and limitations on use of procedural mechanisms to implement role separation, are described below for each level of assurance:

Table 5-1 Role Separation Rules

Assurance Level	Role Separation Rules
Rudimentary	No stipulation
Basic	Individual personnel must be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume more than one role; however, no one individual shall assume both the Officer and Administrator roles. This may be enforced procedurally. No individual shall be assigned more than one identity.

Table 5-1 Role Separation Rules

Assurance Level	Role Separation Rules
Medium and Medium Hardware	Individual personnel must be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume only one of the Officer, Administrator, and Auditor roles, but any individual may assume the Operator role. The CA, CMS, and RA software and hardware must identify and authenticate its users and must ensure that no user identity can assume both an Administrator and an Officer role, assume both the Administrator and Auditor roles, or assume both the Auditor and Officer roles. No individual may have more than one identity.
High	Individual personnel must be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume only one of the Officer, Administrator and Auditor roles. Individuals designated as Officer or Administrator may assume the Operator role. An auditor may not assume any other role. The CA and RA software and hardware must identify and authenticate its users and must enforce these roles. No individual shall have more than one identity.

A Trusted Role may perform the same role on the CA, and KED.

Under no circumstances will a KRA or KRO be an Administrator or Auditor for a KED.

A RA may fill the role of a KRA or KRO. An LRA may fill the role of a KRO.

Only the Auditor Trusted Role may perform internal compliance auditor functions.

The DOS PKI AD Root CA must operate at the High Assurance level. For DOS PKI Subordinate CAs, the applicable CPS designates the operating assurance level.

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Security Clearance Requirements

All persons filling trusted roles must be selected based on loyalty, trustworthiness, and integrity. Trusted persons shall be Department of State direct-hire personnel or contractors. Only U.S. citizens may fill DOS PKI trusted roles.

Only employees of the DOS PKIPO may fill DOS PKI trusted roles, unless specifically appointed by the DOS PKI OA to satisfy operational requirements. In addition to having the required knowledge and experience to perform the trusted role functions, personnel appointed to DOS PKI trusted roles must meet the following requirements:

- Be employees of the Department of State, GS-5 (equivalent) or above, or equivalent contractor/vendor position of responsibility
- Must be a U.S. citizen
- Have not been previously relieved of related duties for reasons of negligence or non-performance of duties
- Have not been denied a security clearance, or had a security clearance revoked
- Have not been convicted of a felony offense
- Be appointed in writing by the DOS PKI OA
- Must hold at a minimum a SECRET security clearance
- Undergo role specific training in accordance with Section 5.5.3.

5.3.2 Background Check Procedures

DOS PKI personnel acting in PKI trusted roles must, at a minimum, undergo background check procedures necessary to be cleared at the SECRET level as outlined in 3 FAM 2222. Information obtained from such checks, performed solely to determine the suitability of a person to fill a DOS PKI role, are not releasable except as required in Section 9.4.

DOS PKI CA personnel must receive a favorable adjudication after undergoing a background investigation covering the following areas::

- Employment
- Education
- Place of residence
- Law Enforcement, and
- References

The period of investigation must cover at least the last five years for each area, excepting the residence check, which must cover at least the last three years. Regardless of the date of award, the investigation must verify the highest educational degree obtained.

Adjudication of the background investigation must be performed by a competent adjudication authority using a process consistent with [Executive Order 12968] or equivalent.[17]

If a formal clearance is the basis for background check, the background refresh must be in accordance with the corresponding formal clearance. Otherwise, the background check must be refreshed every ten years.

[17] A successfully adjudicated National Agency Check with Written Inquires (NACI) or National Agency Check with Law Enforcement Check (NACLC) on record is deemed to have met the minimum standards specified above.

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of a DOS PKI CA or RA must receive comprehensive training..

Training must be conducted in the following areas:

- CA (or RA) security principles and mechanisms,
- Key Recovery System security principles and mechanisms,
- All PKI software versions in use on the CA (or RA) system,
- All PKI duties they are expected to perform,
- Disaster recovery and business continuity procedures, and
- Stipulations of the applicable CP and CPS.

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

5.3.4 Retraining Frequency and Requirements

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

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

5.3.5 Job Rotation Frequency and Sequence

This policy makes no stipulation regarding frequency or sequence of job rotation. Local policies that do impose such requirements must provide for continuity and integrity of the PKI service. Job rotation must not violate role separation. All access rights associated with a previous role must be terminated.

All job rotations must be documented. Individuals assuming an auditor role must not audit their own work from a previous role.

5.3.6 Sanctions for Unauthorized Actions

The DOS PKI OA must take appropriate administrative and disciplinary actions against personnel who have performed actions involving the DOS PKI CAs, RAs, KRSs, CSSs, or repositories not authorized in this CP, the applicable CPS, or other procedures documented by the DOS PKI OA.

A CMA must report suspected security violations or compromises to Diplomatic Security and the DOS PKI OA so that the proper authorities may take appropriate administrative and/or disciplinary actions against personnel who violate the applicable provisions of 12 FAM 590.

5.3.7 Independent Contractor Requirements

Contractor personnel employed to operate any part of the DOS PKI or perform functions pertaining to the Department's PKI infrastructure must be subject to the same requirements as U.S. Government employees performing those functions. Contractor personnel filling trusted roles must be cleared at a minimum to the SECRET level in accordance with 12 FAM 570 and 3 FAM 2222.

5.3.8 Documentation Supplied to Personnel

The DOS PKIPO must provide documentation to each person assigned to a DOS PKI Trusted Role to provide the information they need to perform the functions of that role, including relevant policies and practices, roles and responsibilities, operating procedures, architecture and system information, and security and contingency plans.

5.4 AUDIT LOGGING PROCEDURES

The objective of audit log processing is to review all actions to ensure they are made by authorized parties and for legitimate reasons.

At a minimum, audit records must be generated for all applicable events identified in Section 5.4.1 of this policy and must be available during audit reviews and third-party audits. For CAs operated in a virtual environment, audit records must be generated for all applicable events on application software and all system software layers.

Where possible, the security audit logs must be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism must be used. All security audit logs, both electronic and non-electronic, must be retained and made available during compliance audits. Implementation and documentation of automated tools must describe how relevant events and anomalies are recorded.

Audit record reviews should be performed using an automated process and must include verification that the logs have not been tampered with, an inspection of log entries, and a root cause analysis for any alerts or irregularities.

A record of the review, all significant events, and any actions taken as a result of these reviews must be explained in an audit log summary. This review summary must be retained as part of the long-term archive.

When Key Escrow and Recovery is supported, all KED audit records of unsuccessful key recoveries must be analyzed to determine the cause and to ensure that the KRS is operating correctly and securely and is not vulnerable to unauthorized use.

Real-time alerts are neither required nor prohibited by this policy.

5.4.1 Types of Events Recorded

The following requirements apply to all DOS PKI CAs.

All security auditing capabilities of CA operating system and CA applications required by this CP must be enabled during installation. At a minimum, each audit record must include the following (either recorded automatically or manually for each auditable event):

- What type of event occurred
- Date and time when the event occurred
- Where the event occurred (e.g., on what systems or in what physical locations)
- Source of the event
- Outcome of the event to include success or failure. and
- Identity of any individuals, subjects, or objects/entities associated with the event.

Any request or action requiring the use of a private key controlled by the CA is an auditable event.

If out-of-band processes are used for authorization of certificate issuance, external artifacts from the process (e.g., forms, emails, etc.) must be recorded.

The CA and KRS must record the events identified in the table below, where applicable to the application, environment, or both. Where these events cannot be electronically logged, electronic audit logs must be supplemented with physical logs as necessary.

Table 5-2 Auditable Event Requirements

Auditable Event	Rudimentary	Basic	Medium (All Policies) & High
SECURITY AUDIT			
Any changes to the Audit parameters, e.g., audit frequency, type of event audited		X	X
Any attempt to delete or modify the Audit logs		X	X
IDENTIFICATION AND AUTHENTICATION			
Platform or CA application-level authentication attempts		X	X

Auditable Event	Rudimentary	Basic	Medium (All Policies) & High
The value of maximum authentication attempts is changed		X	X
The number of unsuccessful authentication attempts exceeds the *maximum authentication attempts* during user login		X	X
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts		X	X
An Administrator changes the type of authenticator, e.g., from smart card login to password		X	X
DATA ENTRY AND OUTPUT			
Any additional event that is relevant to the security of the CA (such as remote or local data entry or data export); must be documented		X	X
KEY GENERATION			
Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)	X	X	X
PRIVATE KEY LOAD AND STORAGE			
The loading of CA, RA, CSS, CMS, or other keys used by the CA in the lifecycle management of certificates	X	X	X
All access to certificate subject private keys retained within the CA for key recovery purposes	X	X	X
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE			
Any changes to public keys used by components of the CA to authenticate other components or authorize certificate lifecycle requests (e.g., RA or CMS trust stores)	X	X	X
PRIVATE AND SECRET KEY EXPORT			

Auditable Event	Rudimentary	Basic	Medium (All Policies) & High
The export of private and secret keys (keys used for a single session or message are excluded)	X	X	X
CERTIFICATE REGISTRATION			
All records related to certificate request authorization, approval and signature, whether generated directly on the CA or generated by a related external system or process	X	X	X
CERTIFICATE REVOCATION			
All records related to certificate revocation request authorization, approval and execution, whether generated directly on the CA or generated by a related external system or process		X	X
CERTIFICATE STATUS CHANGE APPROVAL			
All records related to certificate status change request authorization, approval and execution, whether generated directly on the CA or generated by a related external system or process		X	X
CA CONFIGURATION			
Any security-relevant changes to the configuration of the CA. The specific configuration items relevant to the environment in which the CA operates must be identified and documented.		X	X
ACCOUNT ADMINISTRATION			
Roles and users are added or deleted	X	X	X
The access control privileges of a user account or a role are modified	X	X	X
CERTIFICATE PROFILE MANAGEMENT			
All changes to the certificate profile	X	X	X
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT			

Auditable Event	Rudimentary	Basic	Medium (All Policies) & High
All changes to the certificate revocation list profile		X	X
MISCELLANEOUS			
Record of an individual being added or removed from a trusted role, and who added or removed them from the role	X	X	X
Installation of the Operating System		X	X
Installation of the CA		X	X
Installing hardware cryptographic modules			X
Removing hardware cryptographic modules			X
Destruction of cryptographic modules		X	X
System Startup		X	X
Logon Attempts to CA Applications		X	X
Receipt of Hardware/Software			X
Attempts to set passwords		X	X
Attempts to modify passwords		X	X
Backing up CA internal database		X	X
Restoring CA internal database		X	X
Records of manipulation of critical files (e.g., creation, renaming, moving), critical files will vary between installation, and must be identified in the relevant documentation			X
Posting of any material to a repository			X
The date and time any CA artifact is posted to a public repository			X
Access to CA internal database			X

Auditable Event	Rudimentary	Basic	Medium (All Policies) & High
All certificate compromise notification requests		X	X
Loading tokens with certificates			X
Shipment and receipt of tokens containing key material, or tokens that allow access to key material (e.g., HSM operator cards)			X
Zeroizing tokens		X	X
Re-key of the CA	X	X	X
Configuration changes to the CA server involving:			
- Hardware		X	X
- Software		X	X
- Operating System		X	X
- Patches		X	X
- Security Profiles			X
PHYSICAL ACCESS / SITE SECURITY			
Personnel Access to room housing CA			X
Access to the CA server		X	X
Known or suspected violations of physical security		X	X
ANOMALIES			
Software Error conditions		X	X
Software check integrity failures		X	X
Equipment failure	X	X	X
Electrical power outages			X

Auditable Event	Rudimentary	Basic	Medium (All Policies) & High
Uninterruptible Power Supply (UPS) failure			X
Network service or access failures that could affect certificate trust			X
Violations of Certificate Policy	X	X	X
Violations of Certification Practice Statement	X	X	X
Resetting Operating System clock		X	X

5.4.2 Frequency of Processing Log

The CMA Information Systems Security Officer (ISSO), as well as the internal Auditors, may review the audit logs in accordance with the table below.

Audit records must be reviewed at least once every month for online CAs that issue certificates at Basic or above. For offline CAs, the audit logs must be reviewed when the system is activated or every 30 days, whichever is later. CSS, CMS, IDMS, and KRS audit log processing frequency shall align with the CA audit log processing frequency.

Table 5-3 Audit Log Review Schedule

Assurance Level	Audit Log Review Schedule
Rudimentary	Only required for cause
Basic	At least once per month (≤ 30 days)
Medium (all policies)	At least once per month (≤ 30 days)
High	At least once every month (≤ 30 days)

For Basic, Medium (all policies), and High, the CMA Administrator must retrieve PKI and operating system audit logs for the PKI Auditor. The Auditor must examine a statistically significant set (a minimum of 33 percent) of security audit data generated by the CA since the last review (where the security ramifications of the category and availability of tools to perform such a review determine the confidence intervals for each category of security audit data), as well as a reasonable search for any evidence of malicious activity.

The review of audit logs involves verifying that the log has not been tampered with, and at a minimum briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs (e.g., discontinuities, data loss). The ISSO and/or auditors must document actions taken because of these reviews, and reported to the DOS PKI PMA, DOS PKI MA, and/or DOS PKI OA and any other appropriate authorities and entities in the same manner as outlined in Sections 8.5.

5.4.3 Retention Period for Audit Logs

For Basic, Medium, Medium Hardware, and High Assurance CAs, the CMA must retain audit logs on-site until reviewed, as well as archiving such logs in the manner described in Section 5.5.

The CMA-equipment must retain the security audit information it generates for at least two months, as outlined in Section 5.4.4, 5.4.5 and 5.4.6, until moved to an appropriate archive facility.

An entity other than the CMA (i.e., officials different from the individuals who, in combination, command the CA signature key) must delete the security audit data from the CMA-equipment.

The CMA must retain security audit data as archive records in accordance with Section 5.5.

5.4.4 Protection of Audit Logs

System configuration and operational procedures must be implemented together to ensure that only authorized individuals may move or archive audit records and that audit records are not modified.

Collection of the audit records from the CA system must be performed by, witnessed by or under the control of trusted roles who are different from the individuals who, in combination, command the CA signature key.

For RA systems, the individual authorized to move or archive records may not hold an RA Trusted Role.

Procedures must be implemented to protect audit records from deletion or destruction before they are reviewed. as described in Section 5.4.2. To protect the integrity of audit records, they must be transferred to a backup environment distinct from the environment where the audit records are generated.

The CMA must implement procedures to transfer the security audit data to secure storage before overwriting or overflow of automated security audit log files.

The security audit data must not be accessible to or opened by any person, or by any automated process, other than those trusted roles that perform or support security audit processing. The CMA must implement CA system configuration and procedural controls to ensure that:

- Only personnel assigned to trusted roles have read access to the logs
- Only authorized people may copy, move, delete, or archive audit logs

- Audit logs are not modified

Procedures must be implemented to protect archived data from deletion or destruction before the end of the security audit data retention period. The entity responsible for archiving PKI records must move security audit data to a safe, secure storage location separate from the CMA-equipment location where the data was generated, pending its transfer to the official archive location.

5.4.5 Audit Log Backup Procedures

Audit records and audit summaries must be backed up at least monthly.

If audit records are stored locally in the system where the events occur, they must be transferred to a backup environment and protected as described in Section 5.4.4. The backup procedure may be automated or manual but must occur no less frequently than the audit log review described in Section 5.4.2.

The process for transferring the audit records to the backup environment must be documented.

5.4.6 Audit Collection System (Internal vs. External)

The audit log collection system may or may not be external to the CA system or KRS.

Audit processes (automated and manual) must be invoked at system (or application) startup and cease only at system (or application) shutdown.

Audit collection systems must be configured such that security audit data is protected against loss (e.g., overwriting or overflow of automated log files).

The audit processe must run independently, and the CMA must not control it in any way, except to control at installation the implementation of audit data generation and collection capabilities.

In the event that the automated audit system fails, and the integrity of the system or confidentiality of the information protected by the system is at risk, the CMA must cease all operations, except for revocation processing, until it can restore the security audit capability. Under these circumstances, the CMA must employ mechanisms to preclude unauthorized CMA functions. The CPS must describe these mechanisms.

5.4.7 Notification to Event-Causing Subject

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

5.4.8 Vulnerability Assessments

CAs must perform routine vulnerability assessments of the security controls described in the applicable policy.

The CMA, system administrator, and other operating personnel must routinely assess whether the CA system or its components have been attacked, breached, or whether attempts occurred to violate the integrity of the certificate management system, including the equipment, physical location, and personnel.

Self-assessment of controls and control effectiveness (e.g., FISMA) must be performed in accordance with the frequency determined by the risk rating of the CA.

Automated vulnerability scans, if executed, should be run no less frequently than required by the risk rating of the component.

The methodology, tools and frequency of the vulnerability assessment must be documented.

The security auditor must review security audit data for events such as repeated failed actions, requests for privileged information, attempted access of system files, requests for escrowed keys, attempted access of escrowed keys, unauthenticated responses, and other suspicious or unusual activity. Security Auditors should check for continuity of the security audit data.

5.5 RECORDS ARCHIVE

5.5.1 Types of Events Archived

CMA archive records[18] must collect and maintain sufficient detail to establish that the DOS PKI CAs were properly operated in accordance with this policy, as well as verifying the validity of any certificate (including revoked and/or expired) issued by the CAs. At a minimum, the following data must be recorded for archive as specified for each assurance level:

Table 5-4 Data Archival Requirements

Data To Be Archived	Rudimentary	All Other Policies
Certificate Policy	X	X
Certification Practice Statement / Key Recovery Practice Statement	X	X
Contractual obligations	X	X
Other agreements concerning operations of the CA or KRS	X	X
System and equipment configuration	X	X
Modifications and updates to system or configuration	X	X

[18] The term “archive” is not to be confused with a routine backup. The archive addressed in this section is a long-term storage of data that is critical as a historical record. See the terms “archive” and “backup” in this document’s Glossary.

Table 5-4 Data Archival Requirements

Data To Be Archived	Rudimentary	All Other Policies
All records related to certificate request authorization, approval and signature, whether generated directly on the CA or generated as part of a related external system or process	X	X
All records related to certificate revocation, whether generated directly on the CA or generated as part of a related external system or process		X
Subscriber identity Authentication data as per Section 3.2.3		X
Documentation of receipt and acceptance of certificates (if applicable)		X
Subscriber Agreements		X
Documentation of receipt of tokens		X
All certificates issued or published	X	X
Record of CA Re-key	X	X
Other data or applications to verify archive contents		X
Audit summary reports generated by internal reviews and documentation generated during third party audits		X
Any changes to the Audit parameters, e.g., audit frequency, type of event audited		X
Any attempt to delete or modify the Audit logs		X
Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)	X	X
All access to certificate subject private keys retained for key recovery purposes	X	X
Changes to trusted public keys used or published by the CA including certificates used for trust between the CA and other components such as CMS, RA, etc.	X	X

Table 5-4 Data Archival Requirements

Data To Be Archived	Rudimentary	All Other Policies
The export of private and secret keys (keys used for a single session or message are excluded)	X	X
The approval or rejection of a certificate status change request		X
Record of an individual being added or removed from a trusted role, and who added or removed them from the role (to include KRA/KRO)	X	X
Destruction of cryptographic modules		X
All certificate compromise notifications		X
Remedial action taken as a result of violations of physical security		X
Violations of Certificate Policy	X	X
Violations of Certification Practice Statement	X	X

5.5.2 Retention Period for Archive

Archive retention periods begin at the key generation event for any CA. For CAs that leverage key-rollover procedures a new retention period begins for each subsequent key generation event.

CAs shall maintain all archived records related to that CA, in an accessible fashion, for 3 years after CA expiration or CA termination.

Individual RA records associated with certificate request authorization, certificate revocation, subscriber authentication, or subscriber certificate acceptance must be maintained for a minimum of 3 years after the subject certificate expiration date. Issuance of new certificates with extended validity periods (i.e., renewal, rekey or modification) supported by existing subscriber authentication records (i.e., authentication using an existing valid certificate) will result in a new retention period for those initial records, based on the new certificate expiration date.

National Archives and Records Administration General Records Schedules [NARA GRS], 5.6 Item 120, defines required enrollment chain-of-trust records, and archive retention periods related to credentials issued in support of HSPD-12.

RA system operations audit records, that include any IT resources that facilitate RA functions, must maintain relevant archives for a minimum of 3 years after RA system replacement or termination.

5.5.3 Protection of Archive

Only authorized users may access the archive. The CMA must maintain a list of people authorized to access the archive.

Only Auditors, as described in Section 5.2, or other personnel specifically authorized by the DOS PKI OA, are permitted to add to or delete records from the archive. Deletion of records identified in Section 5.5.1 before the end of the retention period is not permitted under any circumstances. The CMA must maintain a list of people authorized to modify or delete records from the archive.

Archive media must be stored in a safe, secure storage facility geographically separate from the CA in accordance with its records retention policies. The transfer process between the backup environment and archive location must be documented. Before archiving, the CMA must label archive records with the name, the date, and the classification of the information. The DOS Data Archive Policy and Procedure must contain procedures detailing how to create, package, and send archive information.

If the original media cannot retain the data for the required period, the DOS PKI OA must define a mechanism to transfer the archived data to new media periodically.

In order to ensure that records in the archive may be referenced when required, the CMA must do one of the following:

- Maintain the hardware or software required to process or read the archive records, or
- Define a process to transfer records to a new format or medium when the old format or medium becomes obsolete and verify the integrity of the records after transfer

The CMA and the archive site must not release the contents of the archive except: (1) in accordance with Department policy; or, (2) as required by law (See Sections 9.3 and 9.4). The CMA may release records of individual transactions upon request of any Subscribers involved in the transaction (i.e., originator or recipient), or their legally recognized agents.

The CMA will coordinate with Department Records Management Officials (A/RPS/IPS/PP) to ensure the scheduling and disposition approval by the NARA of all PKI archived records.

5.5.4 Archive Backup Procedures

If archive records are backed up, the CPS or a referenced document must describe how the archive records are backed up and managed.

5.5.5 Requirements for Timestamping of Records

DOS PKI CA archive records must have accurate timestamps when they are created. The time precision must be such that the sequence of events can be determined.

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

5.5.6 Archive Collection System (Internal or External)

The DOS PKI CA systems, or the CMA staff, may collect archive data in any expedient manner, provided the collection process is documented in the associated CPS.

5.5.7 Procedures to Obtain and Verify Archive Information

The DOS Data Archive Policy and Procedure must describe procedures detailing how to create, verify, package, transmit, and store archive information.

The CMA must not release the contents of the archive except as determined by the DOS PKI PMA or as required by law. The CMA or archive site may release records of individual transactions upon request of any Subscribers involved in the transaction, or their legally recognized agents.

5.6 KEY CHANGEOVER

Each CA's signing key must have a validity period as described in Section 6.3.2.

Prior to the end of a CA's signing key validity period, a new CA must be established or a re-key on the existing CA must be performed. This is referred to as key changeover. From that time on, only the new key is used to sign CA and Subscriber certificates. The old private key may continue to be used to sign CRLs and OCSP Responder certificates. If the old private key is used to sign OCSP Responder certificates or CRLs that cover certificates signed with that key, the old key must be retained and protected.

After all certificates signed with the old key have expired or been revoked, the CA may issue a final long-term CRL using the old key, with a nextUpdate time past the validity period of all issued certificates. This final CRL must be available for all relying parties until the validity period of all issued certificates has passed. Once the last CRL has been issued, the old private signing key of the CA may be destroyed.

When a CA performs a key changeover and thus generates a new public key, the CA must notify all CAs, RAs, and Subscribers that rely on the CA's certificate that it has been changed. The CA must do one of the following:

- Generate key rollover certificate, where the new public key is signed by the old private key, and vice versa or
- Obtain a new CA certificate for the new public key from each issuer of the current CA certificate(s)

5.7 COMPROMISE AND DISASTER RECOVERY

CAs must have an incident handling process, which documents any security incidents. Security incidents may include violation or threat of violation to the system, improper usage, malicious or anomalous activity, and violations of the CPS or CP.

5.7.1 Incident and Compromise Handling Procedures

The DOS PKI OA must notify the DOS PKI PMA and the FPKIPA within 24 hours if a DOS PKI CA experiences any the following:

- Suspected or detected compromise of the CA systems
- Physical or electronic penetration of CA systems
- Successful denial of service attacks on CA components
- Any incident preventing the CA from issuing a CRL prior to the nextUpdate time of the previous CRL
- Suspected or detected compromise of a CSS
- Suspected or detected compromise of an RA.

The notification must include preliminary remediation analysis.

Once the incident has been resolved, DOS PKI OA must provide notification directly to the DOS PKI PMA and the FPKIPA which includes detailed measures taken to remediate the incident. The notice must include the following:

1. Which CA components were affected by the incident
2. The CA's interpretation of the incident
3. Who is impacted by the incident
4. When the incident was discovered
5. A complete list of all certificates that may have been issued erroneously or are not compliant with the CP/CPS because of the incident
6. A statement that the incident has been fully remediated.

The DOS PKIPO must reestablish operational capabilities as quickly as possible in accordance with procedures set forth in the DOS PKI CA’s CPS.

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

When computing resources, software, and/or data are corrupted, the affected DOS PKI CAs must respond as follows:

- The DOS PKI OA must post a notice on its web page identifying the incident and provide notification to the FPKIPA. See Section 5.7.1 for contents of the notice.

- Before returning to operation, the CMA must ensure that system integrity has been restored; and must notify the DOS PKI OA, DOS PKI MA, and DOS PKI PMA
- If the CA signature keys are not destroyed, CA operation must be reestablished, giving priority to the ability to generate certificate status information within the CRL issuance schedule specified in Section 4.9.7
- If the CA signature keys are destroyed, CA operation must be reestablished as quickly as possible, giving priority to the generation of a new CA key pair.

5.7.3 Entity (CA) Private Key Compromise Procedures

5.7.3.1 CA Private Key Compromise Procedures

In the event of a CA private key compromise, the following operations must be performed:

- The DOS PKI OA must immediately inform the FPKIPA, and any entities known to be distributing the CA certificate (e.g., in a root store).
- The DOS PKI OA must request revocation of any certificates issued to the compromised CA.
- The DOS PKI OA must generate new keys in accordance with Section 6.1.1.1.

If the CA distributed the public key in a Trusted Certificate, the CA must perform the following operations:

- Generate a new Trusted Certificate.
- Securely distribute the new Trusted Certificate as specified in Section 6.1.4.
- Initiate procedures to notify Subscribers of the compromise.

Subscriber certificates issued prior to compromise of the CA private key may be renewed automatically by the CA under the new key pair (see Section 4.6) or the CA may require Subscribers to repeat the initial certificate application process.

The DOS PKI OA shall investigate and report to the DOS PKI PMA and the FPKIPA what caused the compromise or loss.

The applicable CPS shall document more detailed procedures for responding to compromise of the private key of the DOS PKI AD Root CA and its Subordinate CAs.

5.7.3.2 KRS Private Key Compromise Procedures

In the event that the KED is compromised or is suspected to be compromised, the following operations must be performed:

- Notify the FPKIPA of the compromise
- Provide detail concerning the root cause, operational impact, and initial remediation actions

- Determine the extent of the compromise
- Gain concurrence from the FPKIPA on planned resolution. This may include revocation of certificates associated with the compromised private keys stored in the KED.

If a KRA or KRO certificate is revoked due to compromise, the potential exists for some Subscribers' escrowed keys to have been exposed during a recovery process, the following operations must be performed:

- Audit record review by the audit administrator to identify all potentially exposed escrowed keys.
- Revocation of each of the potentially exposed escrowed keys, according to procedures specified in Section 4.9.3, to include Subscriber notification of the revocation
- Reissuance of the KRA or KRO authentication certificate

The applicable CPS shall document more detailed procedures for responding to compromise of the KRS.

5.7.4 Business Continuity Capabilities after a Disaster

The CA repository system must be deployed to provide 24-hour, 365 day per year availability with high levels of repository reliability.

CAs must have recovery procedures in place to reconstitute the CA after failure.

In the case of a disaster whereby the CA installation is physically damaged, and all copies of the CA signature key are destroyed as a result, the FPKIPA must be notified at the earliest feasible time, and the FPKIPA must take whatever action it deems appropriate.

The applicable CPS shall document more detailed business continuity procedures.

5.8 CA AND RA TERMINATION

Whenever possible, the FPKIPA must be notified at least two weeks prior to the termination of a DOS PKI CA. For emergency termination, DOS PKI CA s must follow the notification procedures in Section 5.7.

In the event the decision is made to terminate a DOS PKI CA, the following must be accomplished prior to termination:

- Notify all cross-certified Entities.
- Revoke any issued certificates that have not expired[19]

[19] If the termination is for convenience, contract expiration, re-organization, or other non-security related reason, and provisions have been made to continue compromise recovery, compliance and security audit, archive, and data recovery services; then neither the terminated CA's certificate, nor certificates signed by that CA, need to be revoked.

- Generate and publish a final long term CRL with a nextUpdate time past the validity period of all issued certificates. This final CRL must be available for all relying parties until the validity period of all issued certificates has passed.
- Once the last CRL has been issued, destroy the private signing key(s) of the DOS PKI CA.
- Transfer all archive data to an archival facility.

The applicable CPS shall document more detailed procedures for termination of the DOS PKI AD Root CA and its Subordinate CAs.

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

Key generation must be performed using a FIPS approved method or equivalent international standard, with the exception of subscriber rudimentary keys. Key generation events should use the configuration that was the basis of the FIPS or other approved standard (e.g., FIPS mode). If the required keys cannot be generated while in an approved configuration, the specific configuration and reason for use of a different method should be documented by the CA.

This policy does not preclude any source of key generated in accordance with the stipulations of this policy and local security requirements. A private key must not appear outside of the cryptographic module in which it was generated unless encrypted for local transmission or for processing or storage by a key recovery mechanism. Section 6.1.1.1 defines requirements for cryptographic modules used for key generation and storage.

6.1.1.1 CA Key Pair Generation

The DOS PKI AD Root CA, subordinate CAs, and CSSs must generate cryptographic keying material used to sign certificates, CRLs or status information in FIPS 140 validated cryptographic modules as specified in Section 6.2.1. Multiparty control is required for CA key pair generation, as specified in Section 5.2.2.

The DOS PKI AD Root and subordinate CAs must document their key generation procedures and generate auditable evidence that the documented procedures were followed. For all levels of assurance, the documentation of the procedures must provide enough detail to show the use of appropriate role separation.

For High, Medium Hardware, and Medium Assurance, an independent third party must validate the execution of the key generation procedures either by witnessing the key generation or by examining the signed and documented record of the key generation.

6.1.1.2 Subscriber Key Pair Generation

The Subscriber, RA, or CA may perform Subscriber key pair generation. If the CA or RA generates Subscriber key pairs, the requirements for key pair delivery specified in Section 6.1.2 must be met.

For certificates at the High and Medium Hardware assurance levels, subscriber key generation must be performed using a validated hardware cryptographic module as specified in Section 6.2.1. For Medium and Basic assurance, either validated software or validated hardware cryptographic modules must be used for key generation as specified in Section 6.2.1.

6.1.1.3 CSS Key Pair Generation

Cryptographic keying material used by CSSs to sign status information must be generated in [FIPS 140] validated cryptographic modules as specified in Section 6.2.1.

6.1.1.4 PIV-I Content Signing Key Pair Generation

The DOS PKI does not issue certificates for PIV-I cards as defined in the FBCA CP.

Note: Requirements for PIV Content Signing Key Pair Generation are addressed in the FCPF CP.

6.1.2 Private Key Delivery to Subscriber

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

When a CA or RA generates keys on behalf of the Subscriber, the CMA must implement mechanisms to ensure that the public/private key pair is securely delivered to the proper Subscriber. Private keys may be delivered electronically or delivered on a hardware cryptographic module.

For High and Medium Hardware assurance, a private key will be generated and must remain within the cryptographic boundary of a cryptographic module. If the CMA generates the key, then the CMA must securely deliver the cryptographic module containing the key to the Subscriber. The CMA must implement procedures to ensure that the cryptographic module is not activated by an unauthorized Entity. The Subscriber must formally acknowledge receipt of the cryptographic module, and the CMA must maintain a record of the Subscriber acknowledgement of receipt.

If the private key is delivered electronically over a network to the Subscriber, it must be through an encrypted and authenticated channel directly to the Subscriber’s cryptographic module.

In all cases, the following requirements must be met:

- Anyone who generates a private signing key for a Subscriber must not retain any copy of the key after delivery of the private key to the Subscriber.
- The private key must be protected from activation, compromise or modification during the delivery process.
- The Subscriber must acknowledge receipt of the private key.
- Delivery must be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers.
    - For hardware modules, accountability for the location and state of the module must be maintained until the Subscriber accepts possession of it.

- For electronic delivery of private keys, the key material must be encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data must be delivered using a separate secure channel.
- For shared key applications, organizational identities, and network devices, also see Sections 3.2 and 3.3.

6.1.3 Public Key Delivery to Certificate Issuer

For DOS PKI CAs operating at the Basic, Medium, Medium Hardware, or High level of assurance, the following requirements apply:

- Where key pairs are generated by the Subscriber or RA, the public key and the Subscriber's identity must be delivered securely in an authenticated manner to the CA for certificate issuance.
- The delivery mechanism must bind the Subscriber's verified identity to the public key. If cryptography is used to achieve this binding, it must be at least as strong as the CA keys used to sign the certificate. Alternatively, this binding may be accomplished through in-person appearance before the RA, LRA or trusted agent.

For Rudimentary Assurance, this CP makes no stipulation.

6.1.4 CA Public Key Delivery to Relying Parties

When a DOS PKI CA updates its signature key pair, the CA must distribute the new public key in a secure fashion to Relying Parties. The CA may distribute the new public key in a self-signed certificate, in a key rollover certificate, or in a new CA (e.g., cross) certificate obtained from the issuer(s) of the current CA certificate(s).

DOS PKI AD Root CA must make its public key available to Relying Parties, for the creation and verification of certification trust paths, in the form of a self-signed public-key certificate. The DOS PKI AD Root CA must deliver this self-signed certificate to Subscribers in a manner commensurate with the security offered by the public key in the certificate. The self-signed certificate must be conveyed to relying parties in a secure fashion to preclude substitution attacks. Acceptable methods include, but are not limited to the following:

- Loading a self-signed certificate onto tokens delivered to Relying Parties via secure mechanisms
- Distribution of self-signed certificates through secure out-of-band mechanisms
- Comparison of certificate hashes against trusted certificate hashes made available via authenticated out-of-band sources (note that hashes posted in-band along with the certificate are not acceptable as an authentication mechanism)
- Downloading certificates from web sites secured with a currently valid certificate of equal or greater assurance level than the certificate downloaded

DOS PKI CAs must sign key rollover certificates with the CA's current private key, so secure distribution is not required.

6.1.5 Key Sizes

RSA PKCS #1, RSASSA-PSS, or ECDSA signature schemes must be used. Additional restrictions on key sizes and hash algorithms are detailed in Tables 6-1 and 6-2. Certificates must contain 2048 bit, 3072 bit, or 4096 bit RSA keys, or 256 or 384 bit elliptic curve keys. CAs that generate certificates and CRLs under this policy must use the SHA-256, SHA-384, or SHA-512 hash algorithm when generating digital signatures.

Table 6-1 CA Key Size and Hash Algorithm Restrictions

	CA Certificates That Expire On Or Before December 31, 2030	CA Certificates That Expire After December 31, 2030
Minimum Key Size	RSA: 2048 Elliptic Curve: 256	RSA: 3072 Elliptic Curve: 256
Hash Algorithm	SHA-256, SHA-384, or SHA-512	SHA-256, SHA-384, or SHA-512

Table 6-2 Subscriber Key Size and Hash Algorithm Restrictions

	Subscriber Certificates That Expire On Or Before December 31, 2030	Subscriber Certificates That Expire After December 31, 2030
Minimum Key Size	RSA: 2048 Elliptic Curve: 256	RSA: 3072 Elliptic Curve: 256
Hash Algorithm	SHA-256, SHA-384, or SHA-512	SHA-256, SHA-384, or SHA-512

Where implemented, CSSs must sign responses using the same signature algorithm, key size, and hash algorithm used by the CA to sign CRLs.

Use of Transport Layer Security (TLS) or another protocol providing similar security to accomplish any of the requirements of this CP must require at a minimum AES (128 bits) or equivalent for symmetric key, and at least 2048 bit RSA or equivalent for the asymmetric keys. After 12/31/2030, use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP must require at a minimum AES (128 bits) or equivalent for the symmetric key, and at least 3072 bit RSA or or equivalent for the asymmetric keys.

KED and DDS keys must be at equal to or stronger than the keys being escrowed.

6.1.6 Public Key Parameters Generation and Quality Checking

For RSA, the CA shall perform partial public key validation as specified in NIST SP 800-89 (Section 5.3.3).

For ECC, public keys must fall within curves defined in Section 7.1.3. Additionally, the CA should confirm the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine as specified in NIST SP 800-56A (Sections 5.6.2.3.3, or 5.6.2.3.4).

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

DOS PKI CAs must certify public keys bound into certificates for use in signing or encrypting, but not both, except as specified below. The use of a specific key is determined by the key usage extension in the X.509 certificate.

All certificates must include a critical Key Usage extension:

- Certificates to be used only for authentication must set only the digitalSignature bit.
- Certificates to be used by Human Subscribers for digital signatures must set the digitalSignature and nonRepudiation bits.
- Certificates that have the nonRepudiation bit set, must not have keyEncipherment bit or keyAgreement bit set.
- Certificates to be used for encryption (RSA) must set the keyEncipherment bit.
- Certificates to be used for key agreement (ECC) must set the keyAgreement bit.
- CA certificates must set only cRLSign and keyCertSign bits.
- OCSP Responder certificates must assert the digitalSignature and/or nonRepudiation bits

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

Subscriber certificates must assert key usages based on the intended application of the key pair. Subscriber certificates to be used for digital signatures (including authentication) must set the *digitalSignature* and/or *nonRepudiation* bits. However, a public-key certificate with key usage set for *digitalSignature* and *keyEncipherment* must not also set for *nonRepudiation*. Certificates issued only for Authentication must only set the *digitalSignature* bit. Certificates to be used for key or data encryption must set the *keyEncipherment* and/or *dataEncipherment* bits. Certificates used for key encryption must set the *keyAgreement* bit if the algorithm is DH and must set the *keyEncipherment* bit if the algorithm is RSA. This restriction does not prohibit use of protocols that provide authenticated connections using key management certificates. Certificates to be used for key agreement must set the *keyAgreement* bit.

Keys associated with Device Subscriber certificates may be used for digital signature (including authentication), encryption, or both. Except for OCSP Responder certificates, device certificates must not assert the nonRepudiation bit.

Group certificates must only set the *digitalSignature* bit.

Rudimentary, Basic, and Medium Assurance Level certificates may include a single key for use with encryption and signature in support of legacy applications. DOS PKI CAs must generate and manage such dual-use certificates in accordance with their respective signature certificate

requirements, except where otherwise noted in this CP. Such dual-use certificates must never assert the non-repudiation key usage bit, and must not be used for authenticating data that will be verified based on the dual-use certificate at a future time.

At all levels of assurance DOS PKI CAs must issue Subscribers two key pairs, i.e., one for key management and one for digital signature, except where operationally necessary (e.g., VPN and web site/application access control). This restriction does not prohibit use of protocols that provide authenticated connections using key management certificates.

For Subscriber certificates issued after June 30, 2019, the Extended Key Usage extension must always be present and must not contain *anyExtendedKeyUsage* {2.5.29.37.0}. Extended Key Usage OIDs must be consistent with key usage bits asserted.

If a certificate is used for authentication of ephemeral keys[20], the Key Usage bit in the certificate must assert the Digital Signature bit and may or may not assert Key Encryption and Key Agreement depending on the public key in the certificate.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

The relevant standard for cryptographic modules is [FIPS 140], *Security Requirements for Cryptographic Modules*. A FIPS 140 Level 1 or higher validated cryptographic module must be used for all cryptographic operations.

Cryptographic modules must be minimally validated to the FIPS 140 level identified in this section.

The table below summarizes the minimum FIPS 140 requirements for cryptographic modules; higher levels may be used.

Table 6-3 Minimum FIPS 140 Validation Requirement for Cryptographic Modules

Assurance Level	CA	CMS & CSS	Subscriber	RA
Rudimentary	Level 1	Level 1	N/A	Level 1
Basic	Level 2	Level 2	Level 1	Level 1
Medium	Level 3 (Hardware)	Level 2 (Hardware)	Level 1	Level 2 (Hardware)

[20] Example: A session key

Table 6-3 Minimum FIPS 140 Validation Requirement for Cryptographic Modules

Assurance Level	CA	CMS & CSS	Subscriber	RA
Medium Hardware	Level 3 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)
High	Level 3 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)

Any pseudo-random numbers used for key generation material must be generated using a FIPS-validated cryptographic module.

6.2.1.1 Custodial Subscriber Key Stores

Custodial Subscriber Key Stores hold keys for several Subscriber certificates in one location. When a collection of private keys for Subscriber certificates are held in a single location, there is a higher risk associated with compromise of that cryptographic module than that of a single Subscriber.

Cryptographic modules for Custodial Subscriber Key Stores at the Rudimentary Assurance Level must be no less than FIPS 140 Level 1 (Hardware or Software). For all other levels, the cryptographic module must be no less than FIPS 140 Level 2 Hardware.

In addition, authentication to the Cryptographic Device in order to activate the private key associated with a given certificate requires authentication commensurate with the assurance level of the certificate.

6.2.2 Private Key Multi-Person Control

For the DOS PKI AD Root CA, the generation, backup, and activation of the private signing key requires action by two or more persons as set forth in Section 5.2.2 of this CP.

For the DOS PKI Subordinate CAs operating at Medium, Medium Hardware, and High Assurance, the generation, backup, and activation of the private signing key requires action by two or more persons as set forth in Section 5.2.2 of this CP.

For the DOS PKI KED escrowing Medium, Medium Hardware, and High Assurance private decryption keys, the generation, backup, and activation of the private key requires action by two or more persons as set forth in Section 5.2.2 of this CP.

Auditable records must be generated for CA private signing key, and KED private decryption key generation, backup, and activation that document that the required multi-person controls were enforced.

The CMA must maintain a list of names of the parties used for multi-person control.

6.2.3 Private Key Escrow

6.2.3.1 Escrow of DOS Root CA and Subordinate CA Private Signature Keys

DOS PKI CA private signature keys must not be escrowed.

6.2.3.2 Escrow of CA Encryption Keys

DOS PKI AD Root CA must not perform any encryption key recovery functions involving encryption keys issued to subordinate CAs. However, if encryption key pairs need to be issued by the AD Root CA covering repository system access or for other purposes, the DOS PKI PMA must publish applicable requirements for that purpose.

Subordinate CAs may escrow any encryption keys whose certificates do not contain the *digitalSignature* key usage bit for the purpose of data recovery.

6.2.3.3 Escrow of Subscriber Private Signature Keys

Subscriber private signature keys must not be escrowed.

6.2.3.4 Escrow of Subscriber Private Encryption and Dual Use Keys

Subscriber private dual use keys must not be escrowed.

If a device/application has a separate key management key certificate, the key management private key may be escrowed. Subordinate CAs may escrow any encryption keys whose certificates do not also contain the *digitalSignature* key usage bit for the purpose of data recovery as described in Section 4.12.1.

Keys in escrow must be protected using cryptography validated to the same FIPS 140 level as the CA. Recovery of keys in escrow must be protected using the same level of strength of technical controls present at the time of initial issuance, which are described in Section 6.1.2.

6.2.4 Private Key Backup

6.2.4.1 Backup of DOS Root CA and Subordinate CA Private Signature Keys

The DOS PKI AD Root CA must back up its private signature key under multi-person control, as specified in Section 5.2.2.

Backup of subordinate CA private signature keys is required to facilitate disaster recovery. Where required by Section 5.2.2, subordinate CAs must back up private signature keys under multi-person control.

The CMA must create backups of the DOS PKI CA private signature keys on separate cryptographic modules. The CMA must create these keys under the same multi-person control as the original signature key. Such backups must create only a single copy of the AD Root CA and

subordinate CA signature key at the primary CA location. The CMA must store at least one copy of the DOS PKI AD Root CA's and each subordinate CA's private signature key at the off-site backup location. The CMA must account for and protect all copies of CA private signature keys in the same manner as the original.

All backup copies of CA private signature keys must reside solely on cryptographic modules of equal strength and validation level as the primary. These levels are detailed in Section 6.2.1.

6.2.4.2 Backup of Subscriber Private Signature Key

The backup, copying or escrow of a Subscriber private signature key, to include role, group, and device/application, is prohibited.

6.2.4.3 Backup of Subscriber Key Management Private Keys

Subordinate CAs may backup Subscriber key management private keys.

Subordinate CAs must encrypt backed up Subscriber key management private keys using an algorithm of a strength consistent with the private key being stored; or stored in a cryptographic module validated at FIPS 140 Level 2.

6.2.4.4 Backup of CSS Private Key

DOS CMAs may backup CSS private keys. If backed up, the CMA must account for and protect all copies in the same manner as the original.

6.2.5 Private Key Archival

DOS CAs must not archive CA or Subscriber private signature keys.

DOS PKI Subordinate CAs may maintain an archive of escrowed Subscriber private key management keys. Such archives must be protected in accordance with Sections 4.12, 5.1, 5.2, and 6.2.1.

6.2.6 Private Key Transfer into or from a Cryptographic Module

DOS PKI CA private keys must be generated by and remain within a FIPS 140 validated cryptographic module as required by Section 6.2.1. At no time must the CA private key exist in plain text outside the cryptographic module..

CA, ands CSS private signature keys may be exported from the cryptographic module only to perform CA key backup procedures as described in Section 6.2.4.

Subscriber private keys must be generated by and remain within a cryptographic module. If escrowed, a copy of the Subscriber's private key management key must be securely transported between the KED and the Subscriber's cryptographic module.

In the event that a CMA transports a private key from one cryptographic module to another, the private key must be encrypted during transport using a FIPS approved algorithm and at a bit strength commensurate with the key being transported.. Private keys must never exist in plain text form outside the cryptographic module boundary.

The system must protect private or symmetric keys used to encrypt other private keys for transport, from disclosure. The protection of these keys must be commensurate with that provided the data protected by the certificate associated with the private key.

6.2.7 Private Key Storage on Cryptographic Module

This CP makes no further stipulation beyond that specified in [FIPS 140].

6.2.8 Method of Activating Private Keys

For the DOS PKI CAs that operate at the Medium, Medium Hardware, or High level of assurance, CA signing key activation requires multiparty control as specified in Section 5.2.2.

Subscribers must use passphrases, PINS, biometric data, or other mechanisms of equivalent authentication robustness to authenticate to the cryptographic module before activating any private key in the cryptographic module for certificates at all levels of assurance. Section 6.4.1 specifies activation data generation requirements. The CMA must distribute activation data in person, or by an accountable method to the Subscribers separately from the cryptographic modules that they activate. Subscribers must protect the entry of activation data from disclosure using protections described in Section 6.4.2.

For certificates issued under the *mediumDevice* and *mediumDeviceHardware* policy OIDs, the device may be configured to activate its private key without requiring the PKI Sponsor to authenticate to the cryptographic module, provided that appropriate physical and logical access controls are implemented for the device and its cryptographic token. The strength of the security controls must be commensurate with the level of threat in the device's environment; and must protect the device's hardware, software, and the cryptographic module and its activation data from compromise.

6.2.9 Methods of Deactivating Private Keys

If a DOS PKI CA's private signing key is located on a removable cryptographic module, the CMA must remove cryptographic module and store it in a secure container when not in use, as specified in Section 5.1.2.

Subscribers must not leave activated cryptographic modules unattended or otherwise open to unauthorized access. When not in active use, they must be deactivated, e.g. via a manual logout procedure, by removing the cryptographic module, or automatically after a period of inactivity as defined in the applicable CA CPS. Subscribers should remove and secure (e.g., under their personal control or in an approved security container) cryptographic modules when not in use.

6.2.10 Method of Destroying Private Keys

Destroying private keys in software cryptographic modules can be accomplished by overwriting the data using a DS-approved utility and procedures. For hardware cryptographic modules, this will likely be accomplished by executing a "zeroize" command. Private key destruction should not require physical destruction of hardware.

Individuals in trusted roles must destroy CA, RA, and CSS private signature keys when no longer needed.

Subscriber private signature keys must be destroyed when no longer needed, or when the certificates to which they correspond expire or are revoked. Individual Subscribers must take hardware tokens to an LRA, RA, or the CMA for zeroizing.

PKI Sponsors must request the assistance of a LRA, RA, or the CMA with the overwriting of software cryptographic modules used by hardware components and applications.

6.2.11 Cryptographic Module Rating

See Section 6.2.1

6.3 OTHER ASPECTS OF KEY MANAGEMENT

Human Subscribers must typically have one key-pair for digital signature, and a separate key-pair for encryption. A single dual-use (digital signature and encryption) key pair is prohibited for Medium Hardware and High Assurance implementations but may be issued on a case-by-case basis for Rudimentary, Basic and Medium Assurance levels. Such dual-use key pairs must be issued only in support of legacy applications as defined in Section 6.1.7.

A Subscriber's digital signature key-pair must never be escrowed, archived, or backed-up, to maintain technical non-repudiation of Subscriber's signatures.

For business continuity reasons, the CA may escrow, archive, or back-up encryption key-pairs.

6.3.1 Public Key Archival

Public key archival must be in accordance with Section 5.5.

6.3.2 Certificate Operational Periods and Key Usage Periods

DOS PKI CAs must not issue Subscriber certificates with validity periods that extend beyond the expiration date of their own certificate and public key. Each DOS PKI CA certificate validity period must extend one user certificate validity period past the last use of the CA private key.

The validity period of a subscriber certificate must not exceed the routine re-key Identity Requirements as specified in Section 3.3.1.

RA, KRA, and KRO key usage periods are as described for Subscribers.

A CA private key may be used to sign CRLs and OCSP responder certificates for the entire usage period of the CA's public key. All certificates signed by a specific CA private key must expire before the end of the usage period for that specific CA's public key. DOS CAs may use their signature key to sign certificates until the end of their private key's usage period. Thereafter, their signing key may only be used to sign CRLs and OCSP Responder certificates until the last Subscriber certificate signed using that key has expired.

All restrictions on private key usage periods must be enforced procedurally or technically.

Table 6-4 specifies the maximum private key usage period and public key usage period (certificate validity period) for the types of certificates issued by the DOS PKI's AD Root CA, and Subordinate CAs.

Table 6-4 Maximum Key Usage Periods for DOS PKI CA, CSS and Subscriber Certificates

CA and Subscriber Certificate Type	Private Key Usage Period	Public Key Usage Period (Certificate Validity Period)
AD ROOT CA		
Self-Signed Certificate	20 years	20 years
Subordinate CA Certificates		
AD HACA Certificate	10 years	10 years
PIV CA2 Certificate	10 years	10 years
DPC CA Certificate**	10 years	10 years
AD HACA (Subordinate CA)		
Administrator Authentication Certificate	3 years	3 years
SNAP Digital Signature Certificate*	3 years	3 years
SNAP Key Management Key Certificate	Unrestricted	3 years
Yubikey Digital Signature certificate	3 years	3 years
Yubikey Key Management Key certificate	3 years	3 years

Table 6-4 Maximum Key Usage Periods for DOS PKI CA, CSS and Subscriber Certificates

CA and Subscriber Certificate Type	Private Key Usage Period	Public Key Usage Period (Certificate Validity Period)
Code Signing Certificate	3 years	3 years
Role-based Digital Signature Certificate*	3 years	3 years
Role-based Key Management Key Certificate	Unrestricted	3 years
Group Digital Signature Certificate*	3 years	3 years
Group Key Management Key Certificate	Unrestricted	3 years
OCSP Responder Certificate	3 years	120 days
Device Certificate	3 years	3 years
Wildcard Certificate	1 year	1 year
PIV CA2 (Subordinate CA)		
FLAC Authentication Certificate	3 years	3 years
FLAC Card Authentication Certificate	3 years	3 years
FLAC Signature Certificate*	3 years	3 years
FLAC Key Management Key Certificate	Unrestricted	3 years
OCSP Responder Certificate	3 years	120 days

* Signatures generated with subscriber signature certificates may be validated after expiration of the certificate.

** Certificates issued by the Subordinate DPC CA are governed by the FCPF CP and therefore are not addressed in this Table.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

The activation data used to unlock DOS PKI AD Root CA, subordinate CA or Subscriber private keys, in conjunction with any other access control, must have an appropriate level of strength for the keys or data protected. If the activation data must be transmitted, it must be via an appropriately protected channel, and separate in time and place from the associated cryptographic module. Where the DOS PKI AD Root CA or a subordinate CA uses passphrases as activation data for the CA signing key, at a minimum the CMA must change the activation data upon CA re-key.

For Medium Assurance and above, for RAs and Subscribers the activation data may be user selected. The activation data used to unlock private keys must have an appropriate level of strength for the keys or data protected. Passphrases, PINS, biometric data, or other mechanisms of equivalent authentication robustness must be used to protect access to a private key[21]. When passphrases are used, they must be a minimum of twelve (12) characters. When PINs are used, they must be a minimum of six (6) characters.

6.4.2 Activation Data Protection

Data used to unlock private keys must be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data must be:

- Memorized
- Biometric in nature, or
- Recorded and secured at the level of assurance associated with the activation of the cryptographic module and must not be stored with the cryptographic module.

The protection mechanism must include the ability to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts as set forth in the respective CPS.

Subscribers must never share activation data for private keys associated with certificates asserting individual identities. PKI Sponsors must restrict activation data for private keys associated with certificates asserting group, organizational, non-human component identities to those in the organization authorized to use the private keys.

If transmission of the activation data must occur, it must be via a channel with appropriate protection, and distinct in time and place from the associated cryptographic module. As part of the delivery method, users must sign and return a delivery receipt. In addition, users will also receive (and acknowledge) a user advisory statement to help them understand their responsibilities for use and control of the cryptographic module.

[21] For certificates issued at the Card Authentication level of assurance, Subscriber authentication is not required to use the associated private key.

6.4.3 Other Aspects of Activation Data

When operating at a Medium Hardware or High assurance level, RAs must change their cryptographic module activation data passphrase at least every six months (180 days)[22].

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

For all DOS PKI CAs, and KEDs, the computer security functions listed below are required. These functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. CAs and ancillary parts must include the following functionality (these functions pertain to all system software layers, where applicable):

- Authenticate the identity of users before permitting access to the system or applications,
- Manage privileges of users to limit users to their assigned roles,
- Generate and archive audit records for all transactions, (see Section 5.4)
- Enforce domain integrity boundaries for security critical processes,
- Require use of cryptography for session communication and database security,
- Require self-test security-related CA services,
- Require a trusted path for identification of all users,
- Provide residual information protection, and
- Require recovery from key or system failure.

For CSS, the computer security functions listed below are required (these functions pertain to all system software layers, where applicable):

- Authenticate the identity of users before permitting access to the system or applications,
- Manage privileges of users to limit users to their assigned roles,
- Enforce domain integrity boundaries for security critical processes,
- Provide residual information protection, and
- Require recovery from key or system failure.

For remote workstations used to administer the CAs, and KEDs, the computer security functions listed below are also required:

- Authenticate the identity of users before permitting access to the system or applications,
- Manage privileges of users to limit users to their assigned roles,

[22] Department of State internal rules regarding changing of "passwords" and "passphrases" differ; the DOS PKI (including PIV CA2 and the DPC CA) use passphrases and adhere to that departmental standard of every six months.

- Generate and archive audit records for all transactions, (see Section 5.4)
- Enforce domain integrity boundaries for security critical processes,
- Provide residual information protection, and
- Require recovery from system failure.

All workstations that are part of the PKI infrastructure must be configured to lock when the smart card or YubiKey token used to authenticate the user is removed from its interface to the workstation.

All communications between any PKI trusted role and any CA must be authenticated and protected from modification.

6.5.2 Computer Security Rating

When evaluated platforms host CA equipment in support of computer security assurance requirements, then the system (hardware, software, and operating system) must operate only in an evaluated and certified configuration, per the Department of State Office of Information Assurance. At a minimum, such platforms must use the same version of the computer operating system as received the evaluation rating.

6.6 LIFE-CYCLE SECURITY TECHNICAL CONTROLS

6.6.1 System Development Controls

The System Development Controls for the DOS PKI CAs (including any remote workstations used to administer the CA) and RAs at the Basic Assurance level and above are as follows:

- Where open-source software has been utilized, the applicant must demonstrate that security requirements were achieved through software verification and validation and structured development/life-cycle management.
- Hardware and software used to administer or operate the CA must be procured and shipped in a fashion to reduce the likelihood that any component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).
- Custom hardware and software must be developed in a controlled environment, and the development process must be defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software.
- The CA hardware and software, including all system software layers, must be dedicated to operating and supporting the CA (i.e., the systems and services dedicated to the issuance and management of certificates). There must be no other applications, hardware devices, network connections, or component software installed which are not part of the CA operation, administration, monitoring and security compliance of the system. CA hardware and system software layers may support multiple CAs and their supporting systems, provided all systems have comparable security controls and are dedicated to the support of the CA in compliance with the same CP.

- Proper care must be taken to prevent malicious software from being loaded onto the CA equipment. All applications required to perform the operation of the CA must be obtained from documented sources. Except for Offline CAs, CA and RA hardware and software must be scanned for malicious code on first use and periodically thereafter.
- Hardware and software updates must be purchased or developed in the same manner as original equipment and must be installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

The configuration of the CA system as well as any modifications and upgrades must be documented and controlled. There must be a mechanism for detecting unauthorized modification to CA software or configuration. The CA software, when first loaded, must be verified as being that supplied from the vendor, with no modifications, and be the version intended for use. The CA must periodically verify the integrity of the software.

6.6.3 Life Cycle Security Controls

This CP makes no stipulation.

6.7 NETWORK SECURITY CONTROLS

This section does not apply to offline CAs.

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

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

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

RAs, CMSs, repositories, CSSs, and remote workstations used to administer the CAs must employ appropriate network security controls. Networking equipment must turn off unused network ports and services. Any network software present must be necessary to the function of the equipment.

Any remote workstation used to administer the CA must use a Virtual Private Network (VPN) to access the CA. The VPN must be configured for mutual authentication, encryption, and integrity. If mutual authentication is shared secret based, the shared secret must be changed at least annually, must be randomly generated, and must have entropy commensurate with the cryptographic strength of certificates issued by the PKI being administered.

The CA must permit remote administration only after successful multi-factor authentication of the Trusted Role at a level of assurance commensurate with that of the CA.

6.8 TIME STAMPING

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

7. CERTIFICATE, CARL/CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

Certificates issued by DOS PKI CAs under this policy must conform to the current version of the Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile [FBCA-PROF].

7.1.1 Version Numbers

Certificates must be of type X.509 v3 (populate version field with integer "2").

7.1.2 Certificate Extensions

Certificates issued by DOS PKI CAs under this policy use standard certificate extensions that must comply with [RFC 5280].

Certificates issued by DOS PKI CAs under this policy must comply with the current version of [FBCA-PROF].

DOS PKI CA certificates must not include critical private extensions.

Subscriber certificates issued by subordinate CAs may include critical private extensions so long as interoperability within the community of use is not impaired.

DOS PKI CA and Subscriber certificates may include any extensions as specified by [RFC 5280] in a certificate, but must include those extensions required by this CP. Any optional or additional extensions must not conflict with the applicable certificate and CRL profiles identified in Section 7.1

7.1.3 Algorithm Object Identifiers

Certificates issued by DOS PKI CAs under this policy must identify the signature algorithm using one of the following OIDs:

Table 7-1 Object Identifiers for Signature Algorithms

Signature Algorithm	Object Identifier
sha256WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 } (1.2.840.113549.1.1.11)
sha384WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12 } (1.2.840.113549.1.1.12)
sha512WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13 } (1.2.840.113549.1.1.13)

Signature Algorithm	Object Identifier
id-RSASSA-PSS	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10 } (1.2.840.113549.1.1.10)
ecdsa-with-SHA256	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2 } (1.2.840.10045.4.3.2)
ecdsa-with-SHA384	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 } (1.2.840.10045.4.3.3)
ecdsa-with-SHA512	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 4 } (1.2.840.10045.4.3.4)

The PSS padding scheme OID is independent of the hash algorithm. The hash algorithm is specified as a parameter (for details, see [PKCS#1]). The following are the approved hash algorithms:

Table 7-2 Object Identifiers for Hash Algorithms for RSA With PSS Padding

Hash Algorithm	Object Identifier
id-sha256	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1 } (2.16.840.1.101.3.4.2.1)
id-sha384	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 2 } (2.16.840.1.101.3.4.2.2)
id-sha512	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 3 } (2.16.840.1.101.3.4.2.3)

Certificates must use the following OIDs to identify the algorithm associated with the subject key:

Table 7-3 Object Identifiers for Public Key Algorithms

Public Key Algorithm	Object Identifier
rsaEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 } (1.2.840.113549.1.1.1)

id-ecPublicKey	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1 } (1.2.840.10045.2.1)

Where non-CA certificates contain an elliptic curve public key, the parameters must be specified as one of the following named curves:

Table 7-4 Object Identifiers for Elliptic Curve

Curve	Object Identifier
ansip256r1	{ iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7 } (1.2.840.10045.3.1.7)
ansip384r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 34 } (1.3.132.0.34)

7.1.4 Name Forms

In general, the DOS PKI will use the X.500 Distinguished Name (DN) in subject and issuer fields of the base certificate throughout the Department of State. Distinguished names must be composed of standard attribute types, such as those identified in [RFC 5280].

The DOS PKI will use HTTP/LDAP-compliant name forms consistent with best practices for AD implementations as defined by the DOS IT-CCB and IRM Enterprise Network Management (IRM/ENM). The applicable CPS must define the use of alternate name forms, when permitted within the system including types, and name constraints.

7.1.5 Name Constraints

Medium, Medium Hardware, and High assurance CA certificates issued by the DOS PKI must impose name constraints and path length constraints as required by [FBCA-PROF].

7.1.6 Certificate Policy Object Identifiers

All certificates issued by the DOS PKI must include a certificate policies extension asserting one or more of the certificate policy OIDs defined by this CP appropriate to the level of assurance with which it was issued. See Section 1.2 for the certificate policies and their associated OIDs that may be asserted under this CP, and to identify the assurance level of each certificate policy.

Delegated OCSP Responder certificates must assert all policy OIDs for which they are authoritative.

7.1.7 Usage of Policy Constraints Extension

The CAs may assert policy constraints in CA certificates. When this extension appears, at least one of r*equireExplicitPolicy* or *inhibitPolicyMapping* must be present. When present, this extension may be marked critical. For Subordinate CA certificates *inhibitPolicyMappings,* skip

certs must be set to 0. For cross-certificates *inhibitPolicyMappings*, skip certs will be set as appropriate. When *requireExplicitPolicy* is included skip certs must be set to 0.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued under this policy may contain policy qualifiers identified in [RFC 5280]. Processing semantics for any critical certificate policy extensions issued to Subscribers must conform to [FBCA-PROF].

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Processing semantics for any critical certificate policy extensions issued to Subscribers must conform to [FBCA-PROF].

7.1.10 Inhibit Any Policy Extension

DOS PKI CAs may assert *InhibitAnyPolicy* in CA certificates. When present, this extension may be marked critical. Skip Certs must be set to 0.

To support legacy applications that cannot process InhibitAnyPolicy, this extension should be marked noncritical, and Skip Certs set to 0.

7.2 CRL PROFILE

7.2.1 Version Numbers

DOS PKI CAs must issue X.509 version two (2) CRLs.

7.2.2 CRL and CRL Entry Extensions

DOS PKI CAs must conform to the CRL profiles addressing the use of each extension as specified in [FBCA-PROF].

7.3 OCSP PROFILE

Certificate Status Servers (CSS) operating under this policy must sign responses using algorithms designated for CRL signing.

The CSS must accept and return SHA-1 hashes when included in the *CertID* and *responderID* fields. The CSS must not return any response containing a hash algorithm in the *CertID* that differs from the *CertID* in the request.

7.3.1 Version Numbers

CSSs operating under this policy must use OCSP version 1.

7.3.2 OCSP Extensions

CSSs operating under this policy must not use critical OCSP extensions.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The DOS PKI and its CAs are subject to an annual review by the FPKIPA to ensure their policies and operations remain consistent with the policy mappings in the cross-certificate issued to the AD Root CA by the FCPCA.

The DOS PKI PMA must have a compliance audit mechanism in place to ensure implementation and enforcement of the requirements of this CP and the applicable CPSs for the DOS PKI CAs. The DOS PKI PMA must ensure that annual audits are conducted for all PKI functions regardless of how or by whom the PKI components are managed and operated.

The DOS PKI must have appropriate authority to operate.

This CP does not impose a requirement for any particular assessment methodology.

8.1 FREQUENCY OF AUDIT OR ASSESSMENTS

The DOS PKI must be subject to a PKI compliance audit at least once per year for High, Medium Hardware, Medium Assurance, and at least once every two years for Basic Assurance. The audit must include all CAs, as well as CSSs, CMSs, RAs, KRAs, and supporting repositories.

Where a status server is specified in certificates issued by a CA, the status server must be subject to the same periodic compliance audit requirements as the corresponding CA. For example, if an OCSP server is specified in the authority information access extension in certificates issued by a CA, that server must be reviewed as part of that CA's compliance audit.

The compliance audit of CAs and RAs and KRAs must be carried out in accordance with the requirements as specified in the *Federal Public Key Infrastructure (FPKI) Annual Review Requirements* [AUDIT] document.

There is no audit requirement for CAs and RAs operating at the Rudimentary level of assurance.

The DOS PKI PMA has the right to require periodic and aperiodic compliance audits or inspections of subordinate CA or RA operations to validate that the subordinate entities are operating in accordance with the security practices and procedures described in their respective CPS, regardless of how or by whom the PKI components are managed and operated.

The FPKIPA has the right to require aperiodic compliance audits of the DOS PKI AD Root CA (and, when needed, DOS PKI subordinate CAs) that interoperate with the FBCA. The FPKIPA must state the reason for any aperiodic compliance audit.

Additionally, the Department of State Office of Information Assurance and/or Bureau of Diplomatic Security Analysis and Certification Division must have the right to require periodic and aperiodic inspections of subordinate CMA operations to validate that the subordinate CMAs are operating in accordance with the security practices and procedures described in the applicable CPS and DOS FAM. The Office of Information Assurance and/or Bureau of

Diplomatic Security Analysis and Certification Division must state the reason for any aperiodic inspection.

8.2 IDENTITY AND QUALIFICATIONS OF ASSESSORS

The auditor must demonstrate competence in the field of compliance audits. At the time of the audit, the CA compliance auditor must be thoroughly familiar with the requirements which the applicable CP imposes on the issuance and management of their certificates. The compliance auditor must perform such compliance audits as a regular ongoing business activity.

The auditor must be a Certified Information System Auditor (CISA), IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

Either the compliance auditor must be a private firm, that is independent from the DOS PKI being audited, or it must be sufficiently organizationally separated from the DOS PKI to provide an unbiased, independent evaluation. An example of the latter would be The DOS Inspector General.

To ensure independence and objectivity, the compliance auditor should not have been:

- Employed by the DOS PKI to participate in the development or operations of the DOS PKI, for a period of at least 5 years prior to the compliance audit
- A significant contributor to the development or maintenance of the DOS PKI CPS(s) that will be used in the compliance audit.

The DOS PKI PMA must approve the selection of the compliance auditor.

The FPKIPA may determine whether a compliance auditor meets this requirement.

8.4 TOPICS COVERED BY ASSESSMENT

The purpose of a compliance audit of a PKI must be to verify that it is operating in accordance with a CPS that meets the requirements of the applicable CP, as well as any MOAs between the PKI and any other PKI. A full compliance audit for the PKI covers all aspects within the scope identified above.

The compliance audit of CAs and RAs and KRAs must be carried out in accordance with the requirements as specified in the *Federal Public Key Infrastructure (FPKI) Annual Review Requirements* [AUDIT] document.

Components other than CAs may be audited fully or by using a representative sample. If the auditor uses statistical sampling, all PKI components, PKI component managers and operators must be considered in the sample. The samples must vary on an annual basis.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

When the compliance auditor finds one or more discrepancies between how the DOS PKI is designed or is being operated or maintained, and the requirements of this CP, applicable MOAs, or the applicable CPSs, the following actions must be performed:

- The compliance auditor must document the discrepancies
- The compliance auditor must promptly notify the DOS PKI OA and provide documentation of the discrepancies
- The DOS PKI OA will report the discrepancies and the proposed corrective actions, including their expected time for completion, to the DOS PKI MA. The DOS PKI PMA must make the final determination of acceptability of the corrective actions.
- The DOS PKI OA and DOS PKI MA must determine what further notifications or actions are necessary to meet the requirements of the DOS PKI CP, its associated CPSs, and any relevant MOA provisions, and then proceed to make such notifications and take such actions without delay
- The DOS PKI OA must ensure that the identified corrective actions are implemented in a timely manner.

When the FPKIPA receives a report of an audit deficiency from DOS PKI, depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the FPKIPA may require additional actions be taken as a condition for continued cross-certification with the FPKI to protect the level of trust in the FPKI infrastructure.

8.6 COMMUNICATION OF RESULTS

On an annual basis, the DOS PKI PMA must submit an annual review package for the DOS PKI to the FPKIPA. This package must be prepared in accordance with the *Federal Public Key Infrastructure (FPKI) Annual Review Requirements* [AUDIT] document and must include an assertion from the DOS PKI PMA that all PKI components have been audited - including any components that may be separately managed and operated. The package must identify the versions of the CPs and CPSs used in the assessment. Additionally, where necessary, the results must be communicated as set forth in Section 8.5 above.

The DOS PKI OA communicates the audit results to the DOS PKIPO staff and to the Diplomatic Security Service/Domestic Operations/Domestic Facilities Protection (DS/DSS/DO/DFP) management that administers the Department’s Personal Identification Card Program. The DOS PKI OA works with them to develop, track progress, and implement corrective actions to address the audit’s deficiency findings.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

The Department currently funds the DOS PKI AD Root and subordinate CAs centrally; however, the DOS PKI PMA reserves the right to charge a fee to external Agencies and internal Bureaus and posts in order to operate the DOS PKI CAs. The CAs will use these fees only to fund operation of the DOS PKI CAs and fielding of PKI hardware and software beyond normally anticipated requirements (e.g., additional and/or special purpose certificates), based on the recommendation of the DOS PKI OA and DOS PKI MA.

9.1.1 Certificate Issuance or Renewal Fees

This CP makes no further stipulation.

9.1.2 Certificate Access Fees

This CP makes no further stipulation.

9.1.3 Revocation or Status Information Access Fee

This CP makes no further stipulation.

9.1.4 Fees for Other Services

This CP makes no further stipulation.

9.1.5 Refund Policy

This CP makes no further stipulation.

9.2 FINANCIAL RESPONSIBILITY

This CP contains no limits on the use of certificates issued by subordinate CAs under this policy, vis-à-vis the protection of financial transactions or information. Entities (e.g., bureaus, offices, posts, missions, external activities), acting as Relying Parties, must determine, within their purview, what financial limits if any they wish to impose for certificates used to consummate a transaction; and must implement applications at an appropriate level of assurance to support those limitations. The DOS PKI PMA and other elements within the Information Resource Management Bureau assume no financial responsibility or liability for those decisions.

9.2.1 Insurance Coverage

This CP makes no further stipulation.

9.2.2 Other Assets

This CP makes no further stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

This CP makes no further stipulation.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

DOS PKI CA information not requiring protection must be made publicly available. The MOA between the DOS PKI and the FPKIPA shall address access to DOS PKI CA information by the Federal PKI Policy Authority. The respective organization, bureau, or post must determine public access to Department information, in accordance with Department policy and Federal law.

9.3.1 Scope of Confidential Information

A certificate must only contain relevant information necessary to effect secure transactions with the certificate. For proper administration of the certificates, a CMA may request non-certificate information for use in managing the certificates within an organization (e.g., identifying numbers, business or home addresses and telephone numbers). The CPS must explicitly identify any such information.

The CMA must handle all information stored locally on the CA equipment and not in the repository as sensitive and restrict access to those with an official need-to-know in order to perform their official duties. The MOA between the DOS PKI and the FPKIPA will address access to DOS information by the FPKIPA.

9.3.2 Information Not Within the Scope of Confidential Information

This CP makes no further stipulation.

9.3.3 Responsibility to Protect Confidential Information

A CMA must not disclose non-certificate information to any third party unless authorized by this policy, required by U.S. law, U.S. government rule or regulation, or order of a U.S. court of competent jurisdiction. The DOS PKI OA must authenticate any request for release of information.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

A Privacy Impact Assessment (PIA) must be conducted by the DOS PKI MA for PKI Systems, and by DS/DSS/DO/DFP for the Identity Management System (IDMS) that supports the issuance of PIV and FLAC Credentials and submitted to the DOS Privacy Office (A/GIS) for approval. If deemed necessary by the DOS Privacy Office, Privacy Plans for the PKI Systems and for the IDMS must be developed, approved and implemented.

9.4.2 Information Treated as Private

DOS PKI CAs must protect all Subscriber's personally identifying information (PII) from unauthorized disclosure. The DOS PKI CAs must also protect personally identifying information for External Entity personnel collected to support cross certification and MOA requirements from unauthorized disclosure. The CMA may release records of individual transactions upon request of any Subscriber (i.e., originator or recipient) involved in the transaction, or their legally recognized agents. The CMA must not release the contents of archives maintained by CAs operating under this policy except as required by law.

The collection of PII must be limited to the minimum necessary to validate the identity of the subscriber. This may include attributes that correlate identity evidence to authoritative sources. The RA/LRA must provide explicit notice to the subscriber regarding the purpose for collecting and maintaining a record of the PII necessary for identity proofing and the consequences for not providing the information. PII collected for identity proofing purposes must not be used for any other purpose.

9.4.3 Information Not Deemed Private

Information included in DOS PKI certificates is not subject to protections outlined in Section 9.4.2.

9.4.4 Responsibility to Protect Private Information

All CMAs must protect personal information from unauthorized disclosure as mandated by the Privacy Act of 1974, as amended. Sensitive information must be stored securely and may be released only in accordance with other stipulations in Section 9.4.

All information collected as part of the identity proofing process must be protected to ensure confidentiality and integrity. If PKI activities are terminated, CMAs must be responsible for disposing of or destroying sensitive information, including PII, in a secure manner, and maintaining its protection from unauthorized access until destruction.

9.4.5 Notice and Consent to Use Private Information

The DOS PKI OA is not required to provide any notice or obtain the consent of the Subscriber or Entity personnel to release private information in accordance with the stipulations of Section 9.4.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The DOS PKI OA must not disclose private information to any third party unless authorized by this policy, required by law, government rule or regulation, or order of a court of competent jurisdiction. Any request for release of information must be processed according to 41 CFR 105-60.605.

9.4.7 Other Information Disclosure Circumstances

This CP makes no further stipulation.

9.5 INTELLECTUAL PROPERTY RIGHTS

The DOS PKI OA will not knowingly violate intellectual property rights held by others. The U.S. Department of State owns any public key certificates and private keys that it issues.

9.6 REPRESENTATIONS AND WARRANTIES

The following obligations pertain to the Department of State DOS PKI PMA, DOS PKI MA, and DOS PKI OA:

- Approve the CPS for each DOS PKI CA that issues certificates under this policy
- Review periodic compliance audits to ensure that DOS PKI CAs are operating in compliance with their approved CPS
- Review name space control procedures to ensure that distinguished names are uniquely assigned for all certificates issued under this policy
- Revise this CP to maintain the level of assurance and operational practicality
- Distribute this CP to all subordinate and cross-certified CAs, all CMAs, and all Subscribers (distribution may be accomplished by making this CP available on a web site)
- Coordinate modifications to this CP to ensure continued compliance by subordinate CMAs operating under approved CPSs
- Review periodic compliance audits to ensure that RAs, CMSs, CSSs and other components operated by subordinate CMAs are in compliance with their approved CPSs.

9.6.1 CA Representations and Warranties

DOS PKI certificates are issued and revoked at the sole discretion of the DOS PKI PMA.

CAs that issues certificates that assert any of the certificate policies defined in this CP must conform to the stipulations of this CP, and must comply with the CPS approved by the DOS PKI PMA for use with this CP.

CAs are ultimately responsible for ensuring that they sign only certificates generated and managed in accordance with this policy.

CAs that issue certificates under this policy are obligated to post all CA certificates and all CRLs in a directory available via a publicly accessible HTTP URI.

9.6.2 RA and KRA Representations and Warranties

An RA or KRA who performs registration or key recovery functions as described in this policy must conform to the stipulations of this policy, and comply with the appropriate CPS approved by the DOS PKI PMA for use with this CP.

RAs or KRAs performing registration or key recovery functions for any DOS PKI CA mapped to the FBCA and/or FCPCA must also comply with the requirements of the MOA between the DOS PKI and the FPKIPA.

An RA or KRA found to have acted in a manner inconsistent with these obligations must be subject to loss of RA and/or KRA privilege, and potentially adverse administrative or disciplinary action under 12 FAM 590.

A CA must ensure that only those who understand the associated Certificate Policy requirements, and who agree to abide by them perform certificate generation, management, revocation, and key recovery functions.

9.6.3 Subscriber Representations and Warranties

For Medium, Medium Hardware and High Assurance levels, a Subscriber must be required to sign a document containing the requirements the Subscriber must meet respecting protection of the private key and use of the certificate before being issued the certificate. For Basic Assurance level, the Subscriber must be required to acknowledge his or her obligations respecting protection of the private key and use of the certificate before being issued the certificate. Whenever possible, subscriber acknowledgement documents may be digitally signed.

Subscribers of DOS PKI CAs at Basic, Medium, and High Assurance Levels must agree to and must be obligated to perform the following:

- Accurately represent themselves in all communications with the PKI authorities and other Subscribers
- Always protect their private keys, in accordance with this policy, as stipulated in their certificate acceptance agreements and local procedures
- Comply with the requirements of this CP and the appropriate CPS, as well as the applicable requirements of the DOS/FPKIPA MOA, as stipulated in their certificate acceptance agreements
- Promptly notify the CMA that issued their certificates upon suspicion of loss or compromise of their private keys. Such notification must be made directly or indirectly through mechanisms consistent with the CA's CPS
- Abide by all the terms, conditions, and restrictions levied on the use of their private keys and certificates
- Use certificates provided by the Department of State PKI only for transactions related to Department of State business.

PKI Sponsors (as described in Sections 3.2.2 and 3.2.3) assume the obligations of Subscribers for the certificates associated with their organizations and hardware components. If the human sponsor for a device is not physically located near the sponsored device, and/or does not have sufficient administrative privileges on the sponsored device to protect the device's private key and ensure that the device's certificate is used only for authorized purposes, the PKI Sponsor may delegate these responsibilities to an authorized administrator for the device. The PKI

Sponsor must document any such delegation in writing; and it must be signed by both the PKI Sponsor and the authorized administrator for the device. Delegation does not relieve the PKI Sponsor of his or her accountability for these responsibilities. The PKI Sponsor must provide a copy (physical or electronic) of all such delegations to the DOS PKI OA.

9.6.4 Relying Party Representations and Warranties

This CP does not specify the steps that a relying party should take to determine whether to rely upon a certificate. The relying party must decide, pursuant to its own policies, what steps to take. The DOS PKI CAs merely provides tools (e.g., certificates, and CRLs) that the relying party may wish to employ in its determination.

9.6.5 Representations and Warranties of Affiliated Organizations

Affiliated Organizations must authorize the affiliation of subscribers with the organization and must inform the Entity CA of any severance of affiliation with any current subscriber.

9.6.6 Representations and Warranties of Other Participants

Third-party key recovery Requestors must formally acknowledge and agree to the obligations described here, prior to receiving a recovered key:

- Requestor must protect Subscribers' recovered key(s) from compromise. Requestor must use a combination of computer security, cryptographic, network security, physical security, personnel security, and procedural security controls to protect their keys and recovered Subscribers' keys.
- Third-Party Requestor must destroy Subscribers' keys when no longer required (i.e., when the data has been recovered).
- Requestor must request and use the Subscriber's escrowed key(s) only to recover Subscriber's data they are authorized to access.
- Requestor must accurately represent themselves to all entities during any key recovery service.
- When the request is made, the Requestor must provide accurate identification and authentication information at least to the same level required for issuing new PKI certificates at the level of the key being requested (e.g., the Requestor sends a digitally signed request using the credential issued by the Entity PKI at the same or higher assurance level as the key being recovered).
- The Third-Party Requestor must protect information concerning each key recovery operation.
- The Third-Party Requestor must communicate information concerning the recovery to the Subscriber when appropriate as determined by the reason for the recovery. The decision to notify the Subscriber must be based on the law and the Issuing Organization's policies and procedures for third party information access.

- In the event that the Third-Party Requestor notifies the Subscriber of a key recovery, the Requestor must consult with the Subscriber to determine whether or not the recovery circumstances warrant revoking the associated public key certificate.
- As a condition of receiving a recovered key, a Requestor must agree to follow the law and the Issuing Organization's policies relating to protection and release of the recovered key.
- Upon receipt of the recovered key(s), the Third-Party Requestor must sign an attestation to the effect:

"I hereby state that I have legitimate and official need to recover this key in order to obtain (recover) the encrypted data that I have authorization to access. I acknowledge receipt of a recovered encryption key associated with the Subscriber identified here [Subscriber Name]. I certify that I have accurately identified myself to the KRO, and truthfully described all reasons that I require access to data protected by the recovered key. I acknowledge my responsibility to use this recovered key only for the stated purposes, to protect it from further exposure, and to destroy all key materials or return them to the KRO when no longer needed. I understand that I am bound by [Issuing Organization] policies, applicable laws and Federal regulations concerning the protection of the recovered key and any data recovered using the key."

9.7 DISCLAIMERS OF WARRANTIES

DOS PKI CAs operating under this policy may not disclaim any responsibilities described herein.

9.8 LIMITATIONS OF LIABILITY

The U.S. Government shall not be liable to any party, except as determined pursuant to the Federal Tort Claims Act (FTCA), 28 U.S.C. 2671-2680, or as determined through a valid express written contract between the Government and another party.

9.9 INDEMNITIES

This CP makes no stipulation.

9.10 TERM AND TERMINATION

9.10.1 Term

This CP becomes effective when approved by the DOS PKI PMA. This CP has no specified term.

9.10.2 Termination

Termination of this CP is at the discretion of the DOS PKI PMA.

9.10.3 Effect of Termination and Survival

The archive requirements of this CP remain in effect through the end of the archive period for the last certificate issued. This CP and its requirements concerning the organization and operations of the DOS PKI infrastructure; certificate application, usage, and revocation; physical and technical security controls; audits; and other business and legal matters must remain in effect through the expiration date of the last certificate issued and/or cessation of operations and closure of the DOS PKI.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

The DOS PKI PMA must establish appropriate procedures for communications with PKIs cross-certified with the DOS PKI via contracts or memoranda of agreement as applicable.

The DOS PKI PMA must communicate to the FPKIPA any planned change to the DOS PKI infrastructure that has the potential to affect the FPKI operational environment at least two weeks prior to implementation. All new artifacts (CA certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the change must be provided to the FPKIPA within 24 hours following implementation.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

The DOS PKI OA must conduct a review of this DOS PKI CP by the DOS PKIPO at least once every year and revise it to incorporate corrections, updates, or changes, as appropriate. The DOS PKI PMA must review the revised CP and approve or reject it. If approved, a copy of the revised CP, with the changes indicated, must be sent to the FPKIPA and any other External Entity Principal CAs cross-certified with the DOS PKI.

DOS entities external to the DOS PKIPO may request changes to the CP by sending them in writing to the DOS PKI OA. The request must include a description of the change, a change justification, and contact information for the person requesting the change. The DOS PKI OA will accept or reject the request based on the results of a review by the DOS PKIPO and notify the requestor.

9.12.2 Notification Mechanism and Period

The DOS PKI MA must send a copy of this DOS PKI CP and subsequent revisions of this DOS PKI CP to CMAs that assert this policy within 5 business days of CP approval. The CMAs will notify Subscribers of any approved changes to the Certificate Policy that directly affect them or their PKI-related responsibilities.

The DOS PKI PMA must make this CP and any subsequent changes to this CP available within 30 days of approval on the following publicly available web site https://pkaps.pki.state.gov/pkiinfo/.

9.12.3 Circumstances Under Which OID Must be Changed

The DOS PKI CAs will change certificate OIDs if the DOS PKI MA or the FPKIPA determines that a change in the CP reduces the level of assurance provided.

9.13 DISPUTE RESOLUTION PROVISIONS

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

The DOS PKI PMA decides any disputes over the interpretation or applicability of the Department of State PKI CP.

9.14 GOVERNING LAW

United States Federal law (statute, case law, or regulation) governs the construction, validity, performance, and effect of certificates issued under this CP for all purposes.

Where an inter-governmental dispute occurs, resolution must be according to the terms of the applicable MOA.

9.15 COMPLIANCE WITH APPLICABLE LAW

The DOS PKI is required to comply with applicable law. See Section 9.14.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

This CP makes no stipulation.

9.16.2 Assignment

This CP makes no stipulation.

9.16.3 Severability

If it is determined that one section of this CP is incorrect or invalid, the other sections must remain in effect until the CP is updated. Section 9.12 describes the requirements for updating this CP. Responsibilities, requirements, and privileges of this document merge into the newer edition upon release of that newer edition.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

This CP makes no stipulation.

9.16.5 Force Majeure

This CP makes no stipulation.

9.17 OTHER PROVISIONS

This CP makes no stipulation.

10. APPENDIX A - REFERENCES

The following documents contain information that is required by reference or that otherwise describes or governs Department of State PKI operation.

Table A-1 References

Reference	Title
12 FAM 600	Information Security Technology, 2000-06-22
41 CFR 105-60	Title 41 Code of Federal Regulations Chapter 105-60 Public Availability of Agency Records and Informational Materials
5 FAM 400	Records Management
ABADSG	Digital Signature Guidelines, 1996-08-01 http://itlaw.wikia.com/wiki/American_Bar_Association_(ABA)_Digital_Signature_Guidelines
APL	Approved Products List (APL) https://www.idmanagement.gov/buy/#products
AUDIT	FPKI Annual Review Requirements https://www.idmanagement.gov/docs/fpki-annual-review-requirements.pdf
CCP-PROF	Common Policy X.509 Certificate and Certificate Revocation List (CRL) Profiles https://www.idmanagement.gov/docs/fpki-x509-cert-profile-common.pdf
CIMC	Certificate Issuing and Management Components Family of Protection Profiles, version 1.0, October 31, 2001.
DS PCI OP	U.S. Department of State Bureau of Diplomatic Security DOS One Badge PIV Card Issuer (PCI) Operations Plan, v1.25 February 14, 2019
Executive Order 12968	Executive Order 12968 - Access to Classified Information https://www.govinfo.gov/content/pkg/FR-1995-08-07/pdf/95-19654.pdf
FAM	U.S. Department of State Foreign Affairs Manual
FBCA CP	X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA), v2.35 April 15, 2019 https://www.idmanagement.gov/docs/fpki-x509-cert-policy-common.pdf

Table A-1 References

Reference	Title
FBCA-PROF	Federal Bridge Certification Authority (FBCA) X.509 Certificate and CRL Extensions Profile https://www.idmanagement.gov/docs/fpki-x509-cert-profiles-fbca.pdf
FCPF CP	X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, v2.2 December 1, 2021 https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-x509-cert-common-policy.pdf
FIPS 140-2	Security Requirements for Cryptographic Modules December 3, 2002. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
FIPS 186-4	Digital Signature Standard, July 19. 2013. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
FIPS 201-3	Personal Identity Verification (PIV) of Federal Employees and Contractors, FIPS 201-3, January 24, 2022. https://csrc.nist.gov/publications/detail/fips/201/3/final
FOIACT	5 U.S.C. 552, Freedom of Information Act. http://www4.law.cornell.edu/uscode/5/552.html
ITMRA	40 U.S.C. 1452, Information Technology Management Reform Act of 1996. https://govinfo.library.unt.edu/npr/library/misc/itref.html
ITU-T X.521	International Telecommunications Union – Telecommunications Standardization Sector (ITU-T) Recommendation X.521 (The Directory: Selected Object Classes), October 14, 2019 https://www.itu.int/rec/T-REC-X.521-201910-I
NS4009	Committee on National Security Systems Instruction (CNSSI) Glossary, March 2, 2022 https://www.cnss.gov/CNSS/openDoc.cfm?b1N63qAnMPTCrJ26SHrOdA==
PA	5 U.S.C. 552a Privacy Act, 1974, as amended

Table A-1 References

Reference	Title
PACS	*Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems*, Version 2.3, The Government Smart Card Interagency Advisory Board's Physical Security Interagency Interoperability Working Group, December 20, 2005. https://www.idmanagement.gov/docs/pacs-tig-scepacs.pdf
PKCS#1	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	Public-Key Cryptography Standards (PKCS) #12: Personal Information Exchange Syntax v1.1 July 2014 https://tools.ietf.org/html/rfc7292
RFC 2510	Certificate Management Protocol, Adams and Farrell, March 1999 https://www.ietf.org/rfc/rfc2510.txt
RFC 2585	Internet X.509 Public Key Infrastructure: Operational Protocols: FTP and HTTP, Russel Housley and Paul Hoffman, May 1999 https://www.ietf.org/rfc/rfc2585.txt
RFC 3647	Certificate Policy and Certification Practices Framework, Chokhani and Ford, Sabett, Merrill, and Wu, November 2003 https://www.ietf.org/rfc/rfc3647.txt
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
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Cooper, Santesson, Farrell, Boeyen, Housley, and Polk, May 2008 http://www.ietf.org/rfc/rfc5280.txt
RFC 5322	Internet Message Format http://www.ietf.org/rfc/rfc5322.txt
RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP https://tools.ietf.org/html/rfc6960

Table A-1 References

Reference	Title
RFC 8551	Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification, J. Schaad, B. Ramsdell, S. Turner, April 2019 https://tools.ietf.org/rfc/rfc8551.txt
SP 800-37	Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, NIST Special Publication 800-37, Revision 2, December 20, 2018 https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
FPKIPA 800-53 Overlay	Federal Public Key Infrastructure Policy Authority (FPKIPA) Security Control Overlay of NIST Special Publication 800-53 Revision 5 Security Controls for Federal PKI Systems, Version 3.0, February 26, 2021 https://www.idmanagement.gov/docs/
SP 800-56A Rev 3	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, NIST Special Publication 800-56A Rev.3. April 16, 2018 https://csrc.nist.gov/publications/detail/sp/800-63/3/final
SP 800-57	Recommendation for Key Management: Part 1- General, NIST Special Publication 800-57 Part 1 Revision 5, May 4, 2020 https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final
SP 800-63-3	Digital Identity Guidelines, NIST Special Publication 800-63-3, March 2, 2020 https://csrc.nist.gov/publications/detail/sp/800-63/3/final
SP 800-73-4	Interfaces for Personal Identity Verification, NIST Special Publication 800-73-4, February 12, 2016 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-73-4.pdf
SP 800-76-2	Biometric Specifications for Personal Identity Verification, NIST Special Publication 800-76-2, July 11, 2013 https://csrc.nist.gov/publications/detail/sp/800-76/2/final
SP 800-78-4	Cryptographic Algorithms and Key Sizes for Personal Identity Verification, NIST Special Publication 800-78-4, May 29, 2015 https://csrc.nist.gov/publications/detail/sp/800-78/4/final

Table A-1 References

Reference	Title
SP 800-79-2	Guidelines for the Accreditation of Personal Identity Verification Card Issuers, NIST Special Publication 800-79-2, July 30, 2015 https://csrc.nist.gov/publications/detail/sp/800-79/2/final
SP 800-89	Recommendation for Obtaining Assurances for Digital Signature Applications, NIST Special Publication 800-89, November 30, 2006 https://csrc.nist.gov/publications/detail/sp/800-89/final
SP 800-157	Guidelines for Derived Personal Identity Verification (PIV) Credentials, NIST Special Publication 800-157, December 19, 2014 https://csrc.nist.gov/publications/detail/sp/800-157/final
X.509	ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

11. APPENDIX B - ACRONYMS AND ABBREVIATIONS

The following table provides a key for acronyms and abbreviations that may appear in this Department of State PKI CP.

Table B-1 Acronyms and Abbreviations

Acronym	Expression
AD	Active Directory
AES	Advanced Encryption Standard
AIA	Authority Information Access
CA	Certification Authority
CAS	Certificate Authority System
CIO	Chief Information Officer
CISA	Certified Information System Auditor
CISO	Chief Information Security Officer
CMA	Certificate Management Authority
CMS	Card Management System
CN	Common Name
CNSS	Committee on National Security Systems
COMSEC	Communications Security
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CRL DP	Certificate Revocation List Distribution Point
CSA	Certificate Status Authority
CSOR	Computer Security Object Registry

Table B-1 Acronyms and Abbreviations

Acronym	Expression
CSS	Certificate Status Server
DN	Distinguished Name
DNS	Domain Name System
DOS	U.S. Department of State
DPC	Derived PIV Credential
DPCI	Derived PIV Credential Issuer
DS	U.S. Department of State Bureau of Diplomatic Security
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ECC	Elliptic Curve Cryptography
ERC	Enhanced Reliability Check
FAM	Foreign Affairs Manual
FAR	Federal Acquisition Regulations
FBCA	Federal Bridge Certification Authority
FCPCA	Federal Common Policy Certification Authority
FCPF	Federal Common Policy Framework
FED-STD	Federal Standard
FIPS	Federal Information Processing Standard
FLAC	Facility Logical Access Card
FPKIMA	Federal Public Key Infrastructure Management Authority
FPKIPA	Federal PKI Policy Authority
FTCA	Federal Tort Claims Act

Table B-1 Acronyms and Abbreviations

Acronym	Expression
GPEA	Government Paperwork Elimination Act of 1998
GS	General Schedule (Federal civilian level)
GSA	General Services Administration
HACA	High Assurance Certification Authority
HTTP	Hypertext Transfer Protocol
HSM	Hardware Security Module
IANA	Internet Assigned Numbers Authority
ICRL	Indirect Certificate Revocation List
IDMS	Identity Management System
ISO	International Organization for Standardization
ISSO	Information Systems Security Officer
IT-CCB	Information Technology - Change Control Board
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunications Sector
ITU-TSS	International Telecommunications Union – Telecommunications System Sector
KED	Key Escrow Database
KRA	Key Recovery Agent or Key Recovery Authority
KRO	Key Recovery Officer
KRP	Key Recovery Policy
KRPS	Key Recovery Practices Statement
LDAP	Lightweight Directory Access Protocol

Table B-1 Acronyms and Abbreviations

Acronym	Expression
LRA	Local Registration Authority
MA	Management Authority
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NACI	National Agency Check with Written Inquiries
NACLC	National Agency Check with Law Enforcement Check
NIST	National Institute of Standards and Technology
NPE	Non-person Entity
NSA	National Security Agency
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PCI	PIV Card Issuer
PE	Person Entity
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification – Interoperable
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509

Table B-1 Acronyms and Abbreviations

Acronym	Expression
PMA	Policy Management Authority
POC	Point of Contact
RA	Registration Authority
RDN	Relative Distinguished Name
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SAN	Subject Alternate Name
SGID	State Global Identifier Database
SHA-X	Secure Hash Algorithm (X: indicates the version number, e.g., Version 1, Version 256)
SIA	Subject Information Access
S/MIME	Secure Multipurpose Internet Mail Extension
SNAP	Secure Network Access with PKI
SO	Security Officer
TA	Trusted Agent
UPN	User Principal Name
UPS	Uninterrupted Power Supply
URI	Universal Resource Identifier
URL	Uniform Resource Locator
U.S.C.	United States Code
UUID	Universally Unique Identifier (defined by RFC 4122)
VME	Virtual Machine Environment

Table B-1 Acronyms and Abbreviations

Acronym	Expression
VPN	Virtual Private Network
WWW	World Wide Web

12. APPENDIX C - GLOSSARY

The following table provides the definitions of selected terms relevant to this Department of State PKI CP.

Table C-1 Glossary

Term	Definition
Access	Ability to make use of any information system (IS) resource. NSTISSI 4009
Access Control	The process of granting or denying specific requests to obtain and use information and related information processing services. [NS4009]
Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Applicant	The Subscriber sometimes also called an "applicant," after applying to a Certification Authority for a certificate, but before the certificate issuance procedure is completed. ABSG footnote 32
Archive	Long-term, physically separate storage.
Attribute Authority	An Entity, recognized by the FPKIPA or comparable Entity body as having the authority to verify the association of attributes to an identity.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies or procedures. [NS4009]
Audit Log	A chronological record of information system activities, including records of system accesses and operations performed in a given period.
Audit Record	An individual entry in an audit log related to an audited event.
Authenticate	To confirm the identity of an Entity when that identity is presented.

Table C-1 Glossary

Term	Definition
Authentication	A security measure designed to protect a communications system against acceptance of fraudulent transmission or simulation by establishing the validity of a transmission, message, originator, or a means of verifying an individual's eligibility to receive specific categories of information. [NS4009]
Backup	Copy of files and programs made to facilitate recovery if necessary. [NS4009]
Binding	Assurance of the integrity of an asserted relationship between items of information that is provided by cryptographic means. [NS4009]
Biometric	A measurable, physical characteristic or personal behavioral trait used to identify, or verify the claimed identity of, an individual. Facial images, fingerprints, and iris image samples are all examples of biometrics.
CA Facility	The collection of equipment, personnel, procedures, and structures that are used by a Certification Authority to perform certificate issuance and revocation.
Card Management System (CMS)	The system that manages the lifecycle of a Smart Card application.
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.
Certificate Management Authority (CMA)	A Certification Authority or a Registration Authority.

Table C-1 Glossary

Term	Definition
Certificate Policy (CP)	A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery, and administration of digital certificates. Indirectly, a Certificate Policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking, and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).
Certificate-Related Information	Information, such as a Subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates.
Certificate Revocation List (CRL)	A list maintained by a Certification Authority of the certificates, which it has issued, that are revoked prior to their stated expiration date.
Certificate Status Server (CSS)	A trusted entity that provides on-line verification to a relying party of a subject certificate's revocation status.
Certification Authority (CA)	An entity authorized to create, sign, issue, and revoke public key certificates.
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).
Client (application)	A system Entity, usually a computer process acting on behalf of a human Subscriber that makes use of a service provided by a server.
Common Criteria	A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.

Table C-1 Glossary

Term	Definition
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction or loss of an object may have occurred. [NS4009]
Computer Security Objects Registry (CSOR)	Computer Security Objects Registry operated by the National Institute of Standards and Technology.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
Containerization	A form of operating system virtualization, through which applications are run in isolated user spaces called containers, all using the same shared operating system (OS).
Cross-Certificate	A certificate used to establish a trust relationship between two Certification Authorities. A certificate issued from a certificate authority (CA) that signs the public key of another CA not within its trust hierarchy that establishes a trust relationship between the two CAs.
Cryptographic Module	A set of hardware, software, and/or firmware that implements approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary of the module
Custodial Subscriber Key Stores	Custodial Subscriber Key Stores hold keys for a number of Subscriber certificates in one location.
Data Integrity	Assurance that the data are unchanged from creation to reception.
Device	A non-person entity, i.e., a hardware device/system or a software application.
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.

Table C-1 Glossary

Term	Definition
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.
End-entity	The Subscriber who is issued a certificate, or a Relying Party who relies on the validity of a certificate.
Entity	Any department, subordinate element of a department, or independent organizational Entity that is statutorily or constitutionally recognized as being part of the Executive Branch of the Federal Government.
Entity CA	A CA that acts on behalf of an Entity and is under the operational control of the Entity.
FPKI Management Authority (FPKIMA)	The Federal Public Key Infrastructure Management Authority is the organization responsible for operating the Federal Bridge Certification Authority and the Federal Common Policy Certification Authority.
Federal Public Key Infrastructure Policy Authority (FPKIPA)	The FPKIPA is a Federal Government body responsible for setting, implementing, and administering policy decisions regarding the Federal PKI Architecture.
Firewall	A part of a computer system or network that is designed to block unauthorized access while permitting outward communication. [NS4009]
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 or virtual machine monitor.
Identity Management System (IDMS)	One or more systems or applications that perform Identity Lifecycle Management functions such as identity proofing, registration, and issuance processes.
Information System Security Officer (ISSO)	Person responsible to the designated approving authority for ensuring the security of an information system throughout its lifecycle, from design through disposal.

Table C-1 Glossary

Term	Definition
Inside threat	A person with authorized access, and thus the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.
Integrity	Guarding against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity. [NS4009] A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage and eventual receipt by the destination.
Intellectual Property	Useful artistic, technical and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Intermediate CA	A CA that is subordinate to another CA and has a CA subordinate to itself.
Key Escrow	The retention of the private component of the key pair associated with a subscriber's encryption certificate to support key recovery. [NS4009] 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 Escrow Database (KED)	The function, system, or subsystem that maintains the key escrow repository and responds to key escrow and key recovery requests from one or more Key Recovery Agents, as specified by this policy.
Key Exchange	The process of exchanging public keys in order to establish secure communications.
Key Generation Material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
Key Pair	Two mathematically related keys having the properties that (i) 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.

Table C-1 Glossary

Term	Definition
Key Recovery	Production of a copy of an escrowed key and delivery of that key to an authorized requestor.
Key Recovery Agent (KRA)	An individual authorized to interface with the key escrow database in conjunction with one or more other key recovery agents) to cause the key escrow database to carry out key recovery requests, as specified by this policy.
Key Recovery Official (KRO)	An individual authorized to authenticate and submit key recovery requests to the Key Recovery Agent on behalf of requestor, as specified by this policy.
Key Recovery Policy (KRP)	A key recovery policy is a specialized form of administrative policy tuned to 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 Practices Statement (KRPS)	A statement of the practices that a Key Recovery System employs in protecting and recovering key management private keys, in accordance with specific requirements (i.e., requirements specified in the KRP).
Legacy PKI	A PKI operated by a Federal Department/Agency that has been cross-certified with the Federal Bridge CA (FBCA) at the Medium Hardware or High Assurance Level.
Local Registration Authority (LRA)	A Registration Authority with responsibility for a local community.
Memorandum of Agreement (MOA)	Agreement between the FPKIPA and an Entity allowing interoperability between the Entity Principal CA and the FBCA and/or FCPCA. Agreement between the DOS PKI and an External Entity PKI allowing interoperability between the two PKIs which is enabled via cross-certification between them.
Modification (of a certificate)	The act or process by which data items bound in an existing public key certificate are changed by issuing a new certificate.
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see authentication).

Table C-1 Glossary

Term	Definition
Naming Authority	An organizational Entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
National Security System	Any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [ITMRA]
Network Guard	An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect with a high degree of assurance, and an external network that is outside the control of the enterprise system,.
Non-Repudiation	Protection against an individual who falsely denies having performed a certain action and provides the capability to determine whether an individual took a certain action, such as creating information, sending a message, approving information, or receiving a message. [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. .
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 identify uniquely each of the policies and cryptographic algorithms supported.
Offline CA	An offline certification authority is a certification authority isolated from network access and is often kept in a powered-down state.
One Badge	The DOS PIV card along with its Facility and Logical Access Card (FLAC) and Facility Access Card (FAC) variants are collectively referred to as the One Badge.

Table C-1 Glossary

Term	Definition
Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).
Outside Threat	An unauthorized Entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.
Physically Isolated Network	A network that is not connected to entities or systems outside a physically controlled space.
PKI Sponsor	A PKI Sponsor fills the role of a Subscriber for groups, organizations, disabled personnel, and non-human system components named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this CP.
Policy Management Authority (PMA)	The individual or group that is responsible for the creation and maintenance of Certificate Policies and Certification Practice Statements, and for ensuring that all Entity PKI components (e.g., CAs, CSSs, Card Management Systems, RAs) are audited and operated in compliance with the entity PKI CP. The PMA evaluates non-domain policies for acceptance within the domain, and generally oversees and manages the PKI certificate policies. The FPKIPA is the PMA for the FBCA and Federal Common Policy Framework CPs. The DOS Deputy Chief Information Officer is the PMA for the DOS PKI CP and has delegated that authority to the Chief of the Systems Integrity (SI) Division.
Principal CA	The Principal CA is a CA designated by an Entity to interoperate with the FBCA and/or FCPCA. An Entity may designate multiple Principal CAs to interoperate with the FBCA and/or FCPCA.
Privacy	Restricting access to Subscriber or Relying Party information in accordance with Federal law.
Private Key	A mathematical key (kept secret by the holder) used to create digital signatures and, depending upon the algorithm, to decrypt messages or files encrypted (for confidentiality) with the corresponding public key.

Table C-1 Glossary

Term	Definition
Public Key	A mathematical key that is publicly available and that applications use to encrypt data or to verify digital signatures created with its corresponding private key.
Public Key Infrastructure (PKI)	The architecture, organization, policies, practices and procedures, server platforms, software and workstations that collectively support the implementation and operation of a certificate-based public key cryptographic system used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	An entity authorized by the certification authority system (CAS) to collect, verify, and submit information provided by potential Subscribers which is to be entered into public key certificates. The term RA refers to hardware, software, and individuals that collectively perform this function.
Re-key (a certificate)	The process of creating a new certificate with a new validity period, serial number, and public key while retaining all other Subscriber information in the original certificate.
Relying Party	A person or Entity that relies on the validity of the binding of the Subscriber's name to a public key to verify or establish the identity and status of an individual, role, system or device; the integrity of a digitally signed message; the identity of the creator of a message; or confidential communications with the Subscriber.
Remote Workstation	In the context of the DOS PKI, ”remote workstation” refers to a system used to access either the system hosting the CA or the CA itself through external networks for maintenance and administration. Note: Reference Section 6.6.1 for additional technical controls required of remote workstations. This term does not refer to consoles within the CA’s security perimeter or to Registration Authority workstations.
Renew (a certificate)	Renewing a certificate means creating a new certificate with a new serial number where all certificate subject information, including the subject public key and subject key identifier, remain unchanged. The new certificate may have an extended validity period and may include new issuer information (e.g., different CRL distribution point, AIA and/or be signed with a different issuer key).

Table C-1 Glossary

Term	Definition
Repository	A system containing data relating to certificates or revocation data as specified in this CP. May refer to a directory, web server, or server which only hosts pre-generated OCSP responses.
Responsible Individual	A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.
Revoke a Certificate	The process of permanently ending the binding between a certificate and the identity asserted in the certificate from a specified time forward, prematurely ending the operational period of the certificate.
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
Risk Tolerance	The level of risk an entity is willing to accept in order to achieve a potential desired result.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Server	A system entity that provides a service in response to requests from clients.
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).
Subscriber	A Subscriber is an Entity that (1) is the subject named or identified in a certificate issued to that Entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual, application or network device.

Table C-1 Glossary

Term	Definition
Superior CA	In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (See subordinate CA).
Supervised Remote Identity Proofing	A real-time identity proofing event where the RA/Trusted Agent is Proofing 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. Supervised Remote Identity Proofing must meet the criteria specified in NIST SP 800-63A Section 5.3.3; and must have the capacity to capture an approved biometric.
System High	The highest security level supported by an information system. [NS4009]
System Software Layer	A layer of software that manages lower layer hardware and software resources and provides services through well-defined interfaces to the higher layers of software. Examples of system software layers are virtual machines, hypervisors, operating systems, and any containerized architectures.
Technical non-repudiation	The contribution public key mechanisms to the provision of technical evidence supporting a non-repudiation security service.
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [NS4009]
Trust List	Collection of trusted certificates used by Relying Parties to authenticate other certificates.

Table C-1 Glossary

Term	Definition
Trusted Agent (TA)	An individual explicitly aligned with one or more registration authority (RA) officers who has been delegated the authority to confirm Subscriber identification during the registration process. A trusted agent (TA) does not have privileged access to certification authority system (CAS) components to authorize certificate issuance, revocation, renewal, modification, or re-key, or key recovery.
Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor."
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
Trustworthy System	Computer hardware, software, and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.
Two-Person Control	Continuous surveillance and control of 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.
Virtual Machine Environment	An emulation of a computer system that provides the functionality of a physical machine in a platform-independent environment. It consists of a host (virtual machine) and isolation kernel (hypervisor) and provides functionality needed to execute entire operating systems.
Wildcard Certificate	A System or Device certificate that contains a wildcard designator (*) in either the common name (CN) in the Subject field or the subjectAltName (SAN) extension or both. A wildcard certificate allows multiple devices to share the same public-private key pair.
Zeroize	A method of erasing electronically stored data by altering or deleting the contents of the data storage so as to prevent the recovery of the data.