United States Department of Defense/ Department of War

X.509 Certificate Policy

Version 11

15 December 2025

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

1 INTRODUCTION

Public Key Infrastructure (PKI) consists of products and services which provide and manage X.509 public key certificates. A public key certificate binds an entity's identity to a particular public/private key pair.

Public key certificates provide security services such as authentication, confidentiality, technical non-repudiation and integrity, and support access control.

1.1 OVERVIEW

The United States (US) Department of Defense (DoD)/Department of War (DoW) X.509 Certificate Policy (CP) is the unified policy under which a Certification Authority (CA) operated by a DoD component is established and operates.

This CP defines the creation and management of public key certificates in support of DoD/DoW PKI (hereafter, simplified to "DoD PKI" in this CP). DoD PKI certificates comply with the [ITU X.509][1] for use in applications requiring communication between networked computer-based systems. Such applications include, but are not limited to, signature of electronic mail and forms; encrypted transmission of unclassified and classified information; and authentication of human or Non-Person Entities (NPEs) such as network equipment, web servers, firewalls, and directories.

This CP does not define a particular implementation of DoD PKI, nor the plans for future implementations or future Certificate Policies. It also does not define certificate policy for CAs operated by external entities on behalf of the DoD.

The network backbone for these network security products may be unclassified networks such as the Internet or Non-classified Internet Protocol Router Network (NIPRNET), Gray network equipment, or classified networks such as the Secret Internet Protocol Router Network (SIPRNET).

> Practice Notes:
>
> DoD Internal NPE PKI on Gray Networks and/or SIPRNET falls under this CP.
>
> Department-wide Internal NPE PKI has been authorized for use on NSS Secret networks managed by DoD. This authorization is based on continued approval by the National Security System (NSS) PKI Member Governing Body (MGB). Initial approval was granted and is reviewed periodically in accordance with [CNSSD506]. Approval can be revoked at the discretion of the NSS PKI MGB. If NSS PKI MGB approval is revoked, DoD Internal NPE as identified in this CP would no longer be authorized under NSS.

This CP is consistent with [RFC 3647].

1.1.1 Certificate Policy

This CP defines the policies governing the issuance, management, and use of [ITU X.509] public key certificates issued under DoD PKI. This CP defines multiple certificate policies, one or more of which may be asserted in a DoD PKI issued certificate by populating the appropriate DoD Certificate Policy Object Identifier(s) (OID) in the *certificatePolicies* extension of the certificate.

All certificates, except self-signed Root CA certificates, issued under this policy shall contain a registered Certificate Policy OID that may be used by a Relying Party to determine the policy under which the certificate was issued.

[1] When [brackets] appear in this document, they designate the short form of document or other found in Section 11 of this document.

1.1.2 Relationship between Certificate Policy and the Certification Practice Statement

This CP states the requirements for issuing and managing certificates that Relying Parties can use in making decisions regarding what assurance they can place in a certificate issued by a DoD PKI CA. Certification Practice Statements (CPSs) state how a DoD PKI member establishes and maintains that assurance.

Each CA that issues certificates under this policy shall have a corresponding approved CPS detailing its technical controls and operating practices. Registration Authorities (RAs), Verifying Officials (VOs) and Trusted Agents (TAs) that support certificate issuance and management processes are subject to the CPS for the CA that is providing certificates. RAs, VOs and TAs may also have a distinct CPS that details the specific policies, processes, and infrastructure under which they operate.

Practices in CPSs may be updated and added to through the process as identified in Section 1.5.4 of this CP.

1.1.3 Scope

The applicability statements in this policy shall be considered minimum requirements; application accreditors may require higher levels of assurance than specified in this certificate policy for the stated applications.

This CP applies to CA and systems that issue certificates that assert this policy and all certificates issued to CAs, other CA components, individual Subscribers, groups/roles, and systems/devices that assert DoD PKI Certificate Policy OID (see Section 1.2). This CP also applies to responsibilities for individuals handling these certificates and persons operating the DoD PKI.

Security management services provided by the PKI include:

- Key Generation/Storage/Recovery;
- Certificate Generation, Update, Renewal, Re-key, and Distribution;
- Certificate Revocation List (CRL) Generation and Distribution;
- Directory Management of Certificate Related Items;
- Certificate token initialization/programming/management;
- Privilege and Authorization Management; and,
- System Management Functions (e.g., security audit, configuration management, archive).

The security of these services is ensured by defining requirements on PKI activities, including (but not limited to) the following:

- 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 and Relying Parties; and,
- Definition of rules to limit liability and to provide a high degree of certainty that the stipulations of this policy are being met.

1.2 DOCUMENT NAME AND IDENTIFICATION

The official title of this CP is *United States Department of Defense/Department of War X.509 Certificate Policy*. When referred to in subordinate CPSs, that name is shortened to “DODCP”.

This CP defines multiple policies. Each policy is assigned an object identifier (OID) to be asserted in certificates issued by CAs that comply with the policy stipulations related to that OID. The OIDs are registered under the id-infosec arc as:

{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) certificate-policy(11)}

id-US-dod-peerInterop	ID::={id-certificate-policy 31}
id-US-dod-mediumNPE-112	ID::={id-certificate-policy 36}

id-US-dod-mediumNPE-128	ID::={id-certificate-policy 37}
id-US-dod-mediumNPE-192	ID::={id-certificate-policy 38}
id-US-dod-medium-112	ID::={id-certificate-policy 39}
id-US-dod-medium-128	ID::={id-certificate-policy 40}
id-US-dod-medium-192	ID::={id-certificate-policy 41}
id-US-dod-mediumHardware-112	ID::={id-certificate-policy 42}
id-US-dod-mediumHardware-128	ID::={id-certificate-policy 43}
id-US-dod-mediumHardware-192	ID::={id-certificate-policy 44}
id-US-dod-admin	ID::={id-certificate-policy 59}
id-US-dod-internalNPE-112	ID::={id-certificate-policy 60}
id-US-dod-internalNPE-128	ID::={id-certificate-policy 61}
id-US-dod-internalNPE-192	ID::={id-certificate-policy 62}

The following policy OIDs are provided as reference for historical purposes. They are no longer authorized (i.e., deprecated) for use in certificates issued under this CP.

id-US-dod-medium	ID::={id-certificate-policy 5}
id-US-dod-mediumHardware	ID::={id-certificate-policy 9}
id-US-dod-PIV-Auth	ID::={id-certificate-policy 10}
Id-US-dod-mediumNPE	ID::={id-certificate-policy 17}
id-US-dod-medium-2048	ID::={id-certificate-policy 18}
id-US-dod-mediumHardware-2048	ID::={id-certificate-policy 19}
id-US-dod-PIV-Auth-2048	ID::={id-certificate-policy 20}

The stipulations in this CP apply to all policy OIDs except *id-dod-peerInterop*, or unless otherwise stated. The *id-dod-peerInterop* OID is only asserted in cross certificates at the direction of the DoD PKI Policy Management Authority (PMA).

The terms Medium Software, Medium NPE, and Medium Hardware are used throughout this CP to refer to groups of policy OIDs with the same requirements as described below. The term “Medium Assurance” refers collectively to Medium-Software, Medium NPE, and Medium-Hardware uses throughout this CP.

All references to Medium Assurance apply to *id-dod-internalNPE*, *id-dod-mediumNPE*, *id-dod-medium*, and *id-dod-mediumHardware* certificates at all key length and bit security levels (as described in [SP 800-57]), unless otherwise stated.

Where a requirement only applies to all NPE OIDs, the requirement will specify NPE. Where a requirement only applies to all *id-dod-internalNPE* OIDs, the requirement will specify Internal NPE. Where a requirement only applies to all *id-dod-mediumNPE* OIDs, the requirement will specify Medium NPE. Where a requirement only applies to all *id-dod-mediumHardware* OIDs, it will specify Medium Hardware.

All NPE certificates shall assert the appropriate Internal NPE or Medium NPE OID. Medium NPE certificates may also assert any Medium Software or Medium Hardware OID if they meet the corresponding requirements.

Requirements (regardless of crypto key size), are the same unless otherwise noted for the following groups of OIDs:

- Internal NPE-112, Internal NPE-128, and Internal NPE-192
- Medium NPE-112, Medium NPE-128, and Medium NPE-192
- Medium-112, Medium-128, and Medium-192
- Medium Hardware-112, Medium Hardware-128, Medium Hardware-192, and Admin

Internal NPE certificates shall only be issued to NPEs and shall be issued by CAs operated under a separate Root CA dedicated to issuing certificates only under the Internal NPE certificate policy OIDs. If Internal NPE certificates are issued on networks operated at different classifications, there will be a separate Root CA for each. CAs that issue certificates for the Internal NPE certificate policy OIDs, shall only contain Internal NPE certificate policy OIDs in their certificates.

Certificates asserting the *id-dod-admin* OID shall only be issued to Subscribers that have been designated to perform system administrator duties within their component or agency.

In order for DoD to issue credentials that meet the requirements of [FIPS 201], the DoD PKI also assert the following certificate policy OIDs in appropriate certificates. These OIDs are from [COMMON]:

id-fpki-common-authentication	ID::= {2 16 840 1 101 3 2 1 3 13}
id-fpki-common-cardAuth	ID::= {2 16 840 1 101 3 2 1 3 17}
id-fpki-common-piv-contentSigning	ID::= {2 16 840 1 101 3 2 1 3 39}

The *id-fpki-common-authentication* and *id-fpki-common-cardAuth* policy OIDs are only asserted in certificates issued on DoD Personal Identity Verification (PIV).[2] The *id-fpki-common-piv-contentSigning* policy OID is only asserted in content signing certificates issued to a card management system that uses the private key to sign data included on the DoD PIV as required by [FIPS 201]. The *id-fpki-common-cardAuth* certificate identifies the PIV card, not the holder of the card. There is no requirement for activation of the private key associated with *id-fpki-common-cardAuth* certificate.

Certificates issued by DoD CAs to CAs shall contain all OIDs for which the subject CA issues certificates. Certificates issued by DoD CAs to Online Certificate Status Protocol (OCSP) Responders shall contain all OIDs used in certificates issued by that CA for which the Responder is authoritative.

The DoD PKI may also assert the following certificate policy OIDs in appropriate certificates. These OIDs are further described in [COMMON]:

id-fpki-common-derived-pivAuth	ID::= {2 16 840 1 101 3 2 1 3 40}
id-fpki-common-derived-pivAuth-hardware	ID::= {2 16 840 1 101 3 2 1 3 41}

The *id-fpki-common-derived-pivAuth* OID meets all of the requirements for DoD Medium Software. The *id-fpki-common-derived-pivAuth-hardware* OID meets all of the requirements for DoD Medium Hardware. There are additional requirements specified in [COMMON] for asserting these OIDs in end entity certificates.

1.3 PKI PARTICIPANTS

The following sections introduce the DoD PKI and community roles involved in issuing and maintaining public key certificates. Trusted for these PKI participants are described in detail in Section 5.2.

Practice Notes:

Under this CP, both CA and RA are identified as Certificate Management Authorities (CMAs). The term CMA is used when a function may be assigned to either a CA or to a RA, or when a requirement applies to both CAs and RAs. The division of Subscriber registration responsibilities between the CA and the RA vary among implementations of this certificate policy. This division of responsibilities shall be described in the CA and RA CPSs.

DoD PKI OCSP Responders that comply with *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP* [RFC 6960] are also considered a CMA if issued a DoD PKI certificate.

The DoD Card Management System (CMS) includes the processes and capabilities that are used by DoD to issue tokens. Both DoD CMS and associated VOs have practices that are approved under this CP using the process as outlined in Section 1.5.4. Compliance requirements for the CMS and VOs are analyzed against the DoD PKI CA and DoD PKI RA requirements in this CP, respectively.

[2] DoD PKI does not issue PIV-Interoperable (PIV-I) certificates. Neither this CP nor its associated CPSs discuss PIV-I requirements, issuing practices, or associated technical specification. CMS references in this document relate to the issuance of certificates to the DoD Common Access Card (CAC) or onto Alternate Tokens (Alt Tokens).

1.3.1 DoD PKI Management

DoD PKI is managed in accordance with DoD Instruction 8520.02, *Public Key Infrastructure and Public Key Enabling* [DoDI 8520.03] and DoD Instruction 8520.03, *Identity Authentication for Information Systems* [DoDI 8520.03].

1.3.1.1 DoD PKI Policy Management Authority (PMA)

DoD PKI is managed by the DoD PKI PMA. The DoD PKI PMA has the following responsibilities:

- oversee the creation and update of certificate policies, including evaluation of changes requested by DoD Services and Agencies, and plans for implementing any accepted changes; provide timely, responsive, DoD Service and Agency coordination to the DoD CP through a consensus-building process;
- review the CPSs of DoD operated CMA and other support activities that offer or provide services to the DoD by analyzing the CPS documents to ensure that the practices of CMAs serving the DoD comply with the DoD PKI Certificate Policies;
- review the results of CMA compliance audits to determine if the CMAs adequately meet the stipulations of approved CPS documents, and make recommendations to the CMAs regarding corrective actions, or other measures that might be appropriate, such as revocation of CMA certificates;
- approve release of audit results to the Federal PKI Policy Authority (PA);
- establish the suitability of non-DoD policies for use within the DoD (for example, in cases where the technical mechanism of "policy mapping" is being considered);
- determine interoperability criteria for external PKI with DoD PKI and approve trust lists; and,
- offer recommendations to the DoD Program and Project Managers and DoD Information System Accreditation Authorities regarding the appropriateness of certificates associated with the DoD certificate policies for specific applications.

DoD PKI PMA decision authority resides with the DoW (CIO)[3] and its designees. The DoD PKI PMA may delegate this authority through appropriate DoD policies and instructions.

1.3.1.2 DoD PKI Program Management Office (PMO)

In accordance with [DoDI 8520.02], DoD PKI PMO manages the following activities:

- DoD PKI X.509 certificate policies and all change proposals;
- DoD PKI CPS for suitability and compliance;
- approval of the DoD Root CA's issuance and modification of CA certificates;
- collection of DoD PKI third-party audit results;
- Operate an offline Root CA (on behalf of the National Security Agency (NSA)) and associated CPSs; and,
- DoD review of all change proposals to the [COMMON] and [FBCA].

1.3.1.3 Defense Information System Agency (DISA)

In accordance with [DoDI 8520.02], DISA manages the following services for DoD PKI:

- management of DoD PKI intermediate and signing CAs and associated CPSs;
- certificate validation services;
- management of repositories of DoD-approved external PKIs;
- posting of DoD PKI Root and Intermediate CA certificates and Certificate Revocation Lists (CRL); and,
- key recovery services

[3] [DoDI 8520.02] Section 2.1 specifies this responsibility as belonging to the DoD CIO; however, in accordance with Secretary of War Memo (20251015), the secondary title of "Chief Information Officer of the DoW" is used for all official actions. As such, "DoW CIO" is used in this CP wherever that role is identified.

1.3.1.4 Department of Defense Manpower Data Center (DMDC)

In accordance with [DoDI 8520.02], DMDC manages the following:

- DoD CMS, including the Real-Time Automated Personnel Identification System (RAPIDS), NIPRNET Enterprise Alternate Token System (NEATS) and the Alternate Token Information Management System (ATIMS) and associated CPSs;
- DoD common access cards (CACs); and,
- RAPIDS VOs and associated CPSs.

1.3.1.5 DoD PKI Certificate Policy Management Working Group

The entity approved under the authority of the DoD Identity, Credential, and Access Management (ICAM) Identity & Credential Management Integration Program Team (IPT) (under the purview of the DoD ICAM Joint Integration Council), with the following responsibilities for DoD:

- development, management, and evaluation of DoD's X.509 CPs and CPSs
- review and recommend approval of CP and CPS updates;
- review results of CPS compliance audits;
- review interoperability between DoD PKI and external PKI communities (including the National Security Systems (NSS) PKI, DISA's External Certification Authority PKI, the Federal PKI, and Five Eyes (FVEY) partner nations).

1.3.1.6 Combatant Command/Service/Agency (CC/S/A) POCs

In accordance with [DoDI 8520.02] (as Component Heads), CC/S/As perform the following roles:

- management of RAs;
- submit addendums to applicable CPSs to capture CC/S/A-specific variations to DoD PKI practices;
- oversee training of CC/S/A RA personnel; and,
- facilitate compliance audits of CC/S/A activities.

CC/S/As POCs participate in the DoD PKI CPMWG as voting members.

1.3.2 Certification Authorities (CAs)

A CA is comprised of the people, services, and systems (hardware and software) authorized by the DoD PKI PMA to create, sign, and issue public key certificates. DoD PKI CAs are ultimately responsible for ensuring that all certificates they sign are generated and managed in accordance with this policy, and shall ensure that certificate generation, management, and revocation functions are performed only by those who understand the associated Certificate Policy OID requirements, and who are obligated to meet them.

Aspects of the issuance and management of DoD PKI certificates include (but is not limited to) the following:

- generation of certificates and CRLs;
- publication of certificates and CRLs;
- renewal, rekey, and revocation of certificates;
- escrow and recovery of Subscriber decryption private keys;
- generation and destruction of CA signing keys;
- performing backups;
- compromise reporting;
- maintaining the CA database;
- hardware cryptographic module programming and management, if appropriate;
- control over the registration process;
- the identification and authentication process; and,
- ensuring that all aspects of the CA services and CA operations and infrastructure related to certificates issued under this policy are performed in accordance with the requirements, representations, and warranties of this policy.

A CA may consist of components such as web servers/portals, databases, signing engines, Certificate Status Server (CSS), Key Generation System, Key Escrow Systems (KES) and internal directories. The requirements stated in this CP applies to all components of the CA.

1.3.3 OCSP Responder

An OCSP Responder that is issued a certificate under DoD PKI is also considered a PKI participant under this CP and is considered a CMA. Specific OCSP Responder requirements are identified throughout this CP.

Primarily, an OCSP Responder is responsible for:

- providing certificate revocation status to the relying parties; and,
- ensuring that revocation status responses provide authentication and integrity services commensurate with the security strength specified as acceptable in Table 4 of [SP 800-57].

1.3.4 Card Management System (CMS)

The DoD PKI Card Management System is responsible for managing smart card token content for all DoD CACs and Alt Tokens. In the context of this policy, CMS requirements are associated with issuance of certificates to the cryptographic module of the DoD CAC or Alt Tokens. VOs are PKI participants who support identity proofing actions as a part of the CMS.

DoD PKI CMSs shall meet the applicable requirements associated with those applicable to the DoD PKI CA as described in this CP unless otherwise specified. VOs shall meet the applicable requirements associated with those applicable to the DoD PKI RA as described in this CP.

1.3.5 Registration Authorities (RAs)

An RA is comprised of the people, services, and systems (hardware and software) authorized by a CA to collect, verify, and submit information provided by potential Subscribers for the purpose of issuing public key certificates. The individuals performing RA functions are acting in a Trusted Role and shall perform those functions in accordance with a CPS approved by the DoD PKI PMA.

Requirements and responsibilities established in this CP applying to Registration Authority shall apply to Local Registration Authorities (LRAs). Any differences in specific registration practices, roles, or responsibilities shall be noted in applicable CPSs.

RA responsibilities include (but are not limited to) the following:

- registering validated Subscribers;
- certificate issuance;
- verifying initial identity, pursuant to Section 3.2.3;
- entering Subscriber information, and verifying correctness;
- securely communicating requests to and responses from the CA;
- receiving and distributing Subscriber certificates;
- verifying the identity and authorization of entities requesting recovery of escrowed key material;
- authorizing and facilitating the recovery of escrowed key material;
- recovering escrowed key material if assigned that responsibility by the DoD PKI;
- performing revocations; and
- performing key recovery operations.

Not all RAs are authorized to perform all RA functions. The specific privileges, duties and responsibilities of individual RAs within the PKI shall be identified in the appointment documentation.

An RA designated to perform key recovery operations may be referred to as a Key Recovery Agent (KRA).

1.3.6 Trusted Agent (TA)

A Trusted Agent (TA) is an individual who has been delegated the authority to perform a portion of the RA function. The use of a TA is optional. A TA shall be explicitly aligned to one or more RAs to perform a portion of the RA functions.

A TA may be authorized to perform the following roles on behalf of the RA:

- record information and verify biometrics of presented credentials for applicants who cannot appear in person;
- other support to Subscribers (specific TA duties, appointment, and limitations shall be stated in the RA CPS).

A TA does not have privileged access to the CA components to authorize certificate issuance.

DoD PKI TAs are designated as holding Trusted Roles.

1.3.7 Subscribers

A Subscriber is the entity whose name appears as the subject in a certificate, and who asserts that it uses its key and certificate in accordance with this policy. A Subscriber may also be issued role-based or group-based certificates. For role- and group-based Subscriber certificates, as well as for all Non-person entity Subscriber certificates, a human PKI Sponsor shall act on behalf of the Subscriber.

DoD PKI Subscribers include entities who have a validated need for a PKI certificate and are authorized by the DoD to receive a certificate to support that validated need. These Subscribers include DoD-authorized individuals, roles, groups, and other NPEs (to include but not limited to systems, equipment, software, applications, and other IT components). All NPEs shall be under the cognizance of humans (i.e., PKI Sponsor), who accept the certificate and are responsible for the correct protection and use of the associated private key.

Practice Notes:

A PKI Sponsor is the individual (human) who fills the role of a Subscriber for NPE and organizations (including groups and roles) that are named as public key certificate subjects.

Role Based Attribute Authorities (RBAA) approve Group/Role Sponsors. Group/Role Sponsors manage certificates issued to members of the Group/Role. These certificates are issued in the interest of supporting accepted business practices. Group-based and Role-based certificates are issued in addition to an individual Subscriber certificate.

CMAs are technically Subscribers to the PKI; however, the term Subscriber as used in this document refers only to non-CMA entities who request certificates.

1.3.8 Relying Parties

A Relying Party is the entity who uses Subscriber's certificate to verify or establish one or more of the following:

- 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
- confidential communications with the Subscriber

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 DoD Relying Parties shall have access to directory services to obtain PKI related information such as the certificates and CRLs.

1.3.9 Third Party Recovery Requestors

In addition to CAs, RAs, and Subscribers, the following Third-Party participants may be authorized to request key recovery:

- DoD officials in a managerial or supervisory role over a Subscriber;
- law enforcement or counterintelligence agents;
- DoD IG and General Counsel;
- agents of U.S. Federal Courts; and,
- any person or organization authorized by the DoD PKI PMA.

1.3.10 Other Participants

CMAs operating under this policy will require the services of other security, community, and application authorities, including those in Trusted Roles such as Compliance Auditors, Security Auditors (i.e., Information System Security Officers (ISSOs), system administrators, and attribute authorities. The CMAs shall identify, in its CPS, the parties responsible for providing such services, and the mechanisms used to support these services. More detail regarding these participants is provided in Section 5.2.

1.4 CERTIFICATE USAGE

DoD PKI supports various security services such as authentication, confidentiality, digital signatures, integrity, and access control. DoD PKI supports the authentication, integrity, and technical non-repudiation security services through digital signatures, and the confidentiality security service through encryption. These basic security services support the long-term integrity of application data, but by themselves may not provide a sufficient integrity solution for all application circumstances.

Certificates asserting a policy OID defined in this CP shall only be used for transactions related to DoD business. CAs must state this requirement in their CPSs and impose a requirement on Subscribers to abide by this limitation.

1.4.1 Appropriate Certificate Uses

The sensitivity of information processed or protected using certificates issued by the DoD PKI varies significantly.

[DoDI 8520.03] specifies types of assurance levels as they relate to [SP 800-63]. [DoDI 8520.03] outlines Identity Assurance Levels (IALs), Authenticator Assurance Levels (AALs), and Federation Assurance Levels (FAL) for use across all of DoD. Minimum standards for IAL and AAL for use as associated with the corresponding appropriate use of a certificate are found in Table 1-1.

Appropriate Use	Minimum IAL (of Subscriber/PKI Sponsor)	Minimum AAL
Common Authentication	IAL3	AAL3
Medium Hardware	IAL3	AAL3
Medium Software	IAL2	AAL2
Medium NPE	IAL2	AAL2
Internal NPE	IAL1	AAL2

Table 1-1

The *id-dod-internalNPE* OIDs shall only be trusted within the DoD. Internal NPE is authorized for use on unclassified and classified networks (to include gray environments).

1.4.2 Prohibited Certificate Uses

Certificates issued under this CP shall not be used other than to support transactions related to U.S. Government business.

DoD PKI certificates issued on the SIPRNET (or any classified environment) shall not be used for communications or access by users or devices on the NIPRNET (or any unclassified environment).

Internal NPE Root CAs shall not be cross certified with any PKI. Internal NPE certificates shall not be used by any system or device for communication with or access by users or devices outside the DoD. Internal NPE certificates authorized for use on classified networks shall not be used by any system or device for communications with or access by users or devices outside of that classified network. Internal NPE certificates authorized for use on gray networks shall not be used by any system or device for communication with or access by users or devices outside of that gray network.

1.5 POLICY ADMINISTRATION

1.5.1 Organization Administering the Document

The DoD PKI PMA is responsible for the definition, revision and promulgation of this policy. The DoD PKI PMA is the Office of the DoW CIO, and its designees.

Technical administration of this document is conducted by the DoD PKI PMO in coordination with the DoD PKI CPMWG.

1.5.2 Contact Person

Questions regarding this CP should be directed to:

DOD PKI PROGRAM MANAGEMENT OFFICE
9800 SAVAGE RD STE 6699
FT GEORGE G MEADE MD 20755-6699

1.5.3 Person Determining CPS Suitability for the Policy

The DoD PKI PMA shall determine the suitability of any CPS to this policy.

The DoD PKI PMA shall commission a compliance analysis study culminating in a written report that provides a summary of areas in which the CPS may not or does not comply with this CP. The compliance analysis shall be performed by an independent party.

The DoD PKI PMA shall determine suitability and approve all Certificate and CRL Profiles.

1.5.4 CPS Approval Procedures

CMAs shall not commence operations without a DoD PKI PMA-approved CPS. Additionally, a CMA shall meet all CP/CPS requirements prior to issuing and/or approving certificates.

To obtain approval of a CPS, a DoD organization shall submit a CPS to the DoD PKI PMA to determine suitability against this CP at the given level of assurance in accordance with Section 1.5.3. In accordance with [DODI 8520.02], all CPSs (and any proposed CPS Addendum) shall be reviewed by the DoD PKI CPMWG for recommendation to the DoD PKI PMA. The DoD PKI PMA shall resolve all discrepancies and any DoD PKI CPMWG concerns prior to approving the CPS.

A CMA may submit an addendum to an approved CPS where a CMA projects minor deviations from established practices and where these differences apply to a specific use case of that CMA. Any proposed addendum is subject to the same approval and review process conducted for CPSs.

Upon approval by the DoD PKI PMA, CPSs shall be made available to DoD entities within the appropriate repository (as controlled items).

All approved CPSs shall be reviewed annually by their respective CMAs. CMAs shall initiate change action to their CPSs and submit to the DoD PKI PMA for an updated approval no later than three years after the previous DoD PKI PMA approval. For CPSs that do not have changes necessitating triennial updating, the DoD PKI PMA may authorize CPSs to remain unchanged.

The DoD PKI PMA is authorized to make the determination that other (non-DoD) CP offer appropriately equivalent levels of assurance to the DoD PKI CP. The DoD PKI PMA may respond to such decisions by methods including but not limited to:

- issuing cross-certificates to other PKIs asserting other policies;
- including certificates issued by other PKIs and asserting other policies, in DoD OCSP Responders; or,
- recommending CAs asserting other policies for inclusion in DoD application trust lists.

The DoD PKI PMA shall make information regarding such equivalency determinations widely available to DoD relying parties.

Updates, modifications, or additions to the Certificate and CRL Profiles shall be submitted via the DoD PKI PMO for consideration by the DoD PKI PMA. Upon approval by the DoD PKI PMA, profiles shall be made available to within the appropriate repository (see Section 2.2).

1.5.5 Waivers

The DoD PKI PMA may grant a waiver to a CMA to meet urgent, unforeseen operational requirements (such as those associated with ongoing military actions or a similar crisis). The DoD PKI PMA shall identify a specific time limit on the waiver not to exceed one year. If the requirement for a variation is required for a longer period, a permanent change to the policy and/or the practice shall be initiated.

If the DoD PKI PMA does not grant a waiver to a CMA, the CMA may submit a request to change the policy including the establishment of a new policy OID.

Any discrepancy between operations of a cross certified CA and the requirements identified in this CP shall be subject to waiver.

1.6 DEFINITIONS AND ACRONYMS

See Section 10.

2 PUBLICATIONS AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

Repositories that support a CA in posting information as required by this policy shall:

- maintain availability of the information as required by the certificate information posting and retrieval stipulations; and,
- provide access control mechanisms sufficient to protect repository information as described in Section 2.4.

The repository that is the primary source of CA certificates and/or CRLs for access by Relying Parties shall be available 24 hours a day, 7 days a week with a minimum overall availability of 99% per year including scheduled down time, which shall not exceed 0.5% per year. Repository availability calculations do not include network down-time.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

Each CA shall provide an on-line repository that is available to Subscribers and Relying Parties. The on-line repository shall contain the following (items that shall be publicly available are indicated accordingly):

- issued encryption certificates that assert this policy;
- CRLs (publicly available);
- CA certificates for certificate signing key (publicly available);
- a copy of any cross-certificate issued by or to the CA (publicly available); and,
- a copy of this policy and associated certificate profiles (publicly available);
- any waivers granted to CAs by the DoD PKI PMA (publicly available).

Additionally, each CA shall provide an on-line repository that is available to Subscribers with certificates asserting this policy that includes sections of the CPS that describes duties and responsibilities.

2.3 TIME OR FREQUENCY OF PUBLICATION

Certificates shall be published following Subscriber acceptance as specified in Section 4.4 and proof of possession of private key as specified in Section 3.2.1. The CRL shall be published as specified in Section 4.9.7. All information to be published in the repository shall be published promptly after such information becomes available to the CA. The CA shall specify in its CPS time limits within which it will publish various types of information.

2.4 ACCESS CONTROLS ON REPOSITORIES

Repository information shall be protected from unauthorized modification and disclosure.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

Names used within DoD shall be associated with the individual, group/role, or NPE for which a certificate is issued. All certificates shall use Distinguished Name (DN) name forms for the issuer and subject name fields. See Section 7 for DN naming conventions.

In general, CAs shall not assign DNs. Subscribers shall have non-null DNs assigned to them through their organizations, in accordance with a naming authority (see Section 3.1.2). The CMA shall investigate and correct, if necessary, any name collisions brought to its attention. If appropriate, the CMA shall coordinate with and defer to the appropriate naming authority. Some certificates may additionally assert an alternate name form. See Section 7.

3.1.2 Need of Names to be Meaningful

Names used within the DoD shall identify the individual, group/role, or NPE to which they are assigned. The CMA shall ensure that an affiliation exists between the Subscriber and any organization that is identified by any component of any name in its certificate.

When DNs are used, the common name shall represent the Subscriber in a way that is easily understandable by humans. For an individual Subscriber the name shall be easily understandable as human. For a group/role Subscriber, the name shall be easily identifiable as associated with a person or organization.

Practice Notes: Individual Subscriber names will typically be a legal name. Group/roles Subscriber names will typically be an established group/role name.

An NPE Subscriber name shall be such that it is not identifiable as a human Subscriber name.

Practice Note: NPE Subscriber names will typically be a fully qualified domain name, IP addresss, model name, serial number, URL, or an application process name.

See Section 7 for DN structure.

Each Root CA asserting this policy shall only sign certificates with subject names from within a name-space approved by the DoD PKI PMA. In the case where one CA certifies another, the certifying CA must impose restrictions on the name space authorized in the subordinate CA, which are at least as restrictive as its own name constraints.

When technical means exist for imposing these constraints (such as the name constraints certificate extension), they shall be used. Otherwise, these constraints shall be imposed procedurally or contractually.

3.1.3 Anonymity or Pseudonymity of Subscribers

A CA shall not issue anonymous certificates. CA certificates shall not contain anonymous or pseudonymous identities.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting DN are specified in [ITU X.501]. Rules for interpreting e-mail addresses are specified in [RFC 5322]. Rules for interpreting the pivFASC-N name type are specified in [PACS].

For applicable certificate profiles, see Section **Error! Reference source not found.**

3.1.5 Uniqueness of Names

Name uniqueness across the DoD shall be enforced.

A CA shall document in its CPS what name forms will be used, how the CA and RAs will interact to guarantee name uniqueness among current and past Subscribers.

3.1.6 Recognition, Authentication and Role of Trademarks

A CMA shall not issue a certificate knowing that it includes a name that a court of competent jurisdiction has determined infringes the trademark of another. A CMA is not obligated to research trademarks or resolve trademark disputes. CMAs may refer trademark disputes to the DoD PKI PMA.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

In all cases where the Subscriber generates keys, the CMA shall verify that the Subscriber has possession of the private key, which corresponds to the public key in the certificate request.

In the case where key generation is performed under the CMA's direct control, proof of possession of the private key is not required.

3.2.2 Authentication of Organization Identity

Requests for certificates in the name of an organization shall include the organization name, address, and documentation of the existence of the organization. The CMA shall verify this information, in addition to the authenticity of the requesting representative, and that representative's authorization to act in the name of the organization. Use of organization certificates shall be addressed in the appropriate CMA CPS. CMAs shall not approve organization certificates when individual non-repudiation is required.

3.2.3 Verification of Individual Identity

All individual identities shall be established by in-person identity proofing. The CMA shall ensure that the applicant's identity information and public key are bound adequately. Each CMA shall specify in its CPS procedures for authenticating a Subscriber's identity. The DoD PKI CA or RA who conducts authentication shall document this action in accordance with Section 5.4.1.

3.2.3.1 In-Person Identity Proofing

In-person identity proofing shall be conducted within 30 days of certificate issuance.

In-person identity proofing shall be established in accordance with the Table 3-1.

Policy	In-Person Identity Proofing Requirement
Internal NPE	No Stipulation
Medium (Software)	Every 9 years
Medium NPE	Every 9 years
Medium Hardware	Every 6 years

Table 3-1

Credentials required to establish individual identity include the following:

- one Federal Government-issued Picture ID; or,
- one REAL ID Act compliant picture ID; or,
- two Non-Federal Government IDs (one of which must be a photo ID).

Any credentials presented shall be unexpired. Any individual conducting identity proofing shall be familiar with anti-tamper and validity features of the documents used for this process.

As an alternative to presentation of identification credentials, 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) may be used.

For Medium Software, Medium NPE, and Medium Hardware, the applicant's identity shall be personally verified prior to the applicant's certificate being enabled. The applicant shall appear personally before either:

- a CMA;
- a TA approved by the CMA; or,
- (for Medium Software only) a person certified by the US Federal Government or a state government as being authorized to confirm identities such as Notaries Public, that uses a stamp, seal or other mechanism to authenticate their identity confirmation. In addition, the CPS shall specify how notification will be provided that this identity proofing has occurred and how it will be verified that the appropriate official performed the identity proofing.

Minors and others not competent to perform face-to-face registration alone shall be accompanied by a person already certified by the PKI, who will present information sufficient for registration at the level of the certificate being requested, for both himself and the person accompanied.

The CMA shall require a signed declaration from the individual (may be handwritten signature or digital signature if biometrically linked to the Subscriber identity). Signature must be applied in the presence of the person performing the identity authentication.

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

For Medium Hardware, Subscribers shall personally appear before the RA or the CMA-approved TA to obtain their tokens or token activation data.

For group/role certificates, Subscriber identity proofing shall use the same methods as that for individual.

3.2.3.2 Electronic Authentication

Medium Assurance certificates may be issued through electronic authentication using a current, valid DoD PKI certificate and associated private key. Subscriber requests shall be subject to the following restrictions:

- the assurance level of the new certificate shall be the same or lower than the assurance level of the existing certificate used as an authentication credential;
- the DN of the new certificate shall be identical to the DN of the signature certificate. Information in the new certificate that could be used for authorization shall be identical to that of the signature certificate;
- the expiration date of the new certificate will be no later than the next required in-person authentication date associated with the signature certificate;
- the in-person authentication date associated with a new certificate will be no later than the in-person authentication date associated with the signature certificate used for authentication; and,
- the validity period of the new certificate shall not be greater than the maximum validity period requirements of this CP for that type of certificate.

Certificates used for electronic authentication need not be revoked.

For certificates that assert one of the *derived-pivAuth* policy OIDs, the issuer shall be approved as a Derived PIV Credential Issuer as specified in [SP 800-79] ". The issuer shall verify that the request for issuance was submitted by an authorized agency employee.

For certificates that assert the *id-fpki-common-derived-pivAuth-hardware* OID, the applicant shall appear in person before an RA who verifies the identity of the applicant by performing a one-to-one comparison of the biometrics stored on the applicants CAC. The biometric samples used in the comparison shall be retained as part of the RA's audit records. The RA shall then observe the applicant authenticate with the PIV-Auth certificate on the applicants CAC.

3.2.3.3 Authentication of NPE Identities

Some NPE (e.g., systems, equipment, software, applications, and other IT component) will be named as certificate subjects.

Except for Internal NPE certificates, the component must have a PKI Sponsor as described in Section **Error! R eference source not found.**. The PKI Sponsor is responsible for providing the CMA correct information regarding:

- NPE identification (e.g., serial number) or service name (e.g., DNS name) or unique software application name;
- NPE public keys;
- NPE authorizations and attributes (if any are to be included in the certificate); and,
- contact information to enable the CMA to communicate with the PKI Sponsor when required.

The CA, or the RA/TA, shall authenticate the identity of the PKI Sponsor and validate their authorization and the integrity of the information. Acceptable methods for performing PKI Sponsor authentication and integrity of information checking include, but are not limited to:

- electronic means (using certificates of equivalent or greater assurance than that being requested); and/or,
- in person registration of the PKI Sponsor, with the identity of the PKI Sponsor confirmed in accordance with the requirements of Section 0.

In the case a PKI Sponsor is changed, the new PKI Sponsor shall review the status of each NPE under his/her sponsorship to ensure it is still authorized to receive certificates.

For Internal NPE certificates, the process shall ensure that:

- an authorized, privileged individual approves connecting the NPE to a DoD network or infrastructure;
- the DoD network or infrastructure authenticates the NPE submitting the certificate request and facilitates authentication of the NPE to the issuing CA; and,
- NPE authorizations, attributes and the specific certificate profile to be applied are validated by the DoD network or infrastructure component that authenticates the request and are provided to the issuing CA in an authenticated manner.

3.2.4 Non-Verified Subscriber Information

All information in certificates that assert a policy OID from [Common] shall be verified.

Subscriber email address included in the certificate (e.g., in the subject alternative name extension) that do not assert a policy OID from [Common] may be unverified.

3.2.5 Validation of Authority

Certificates that contain explicit or implicit organization affiliations shall be issued only after ascertaining the Subscriber has the authorizations to act on behalf of the organization in the implied capacity (e.g., *id-dod-admin* OID certificates, group/role certificates, and CA and RA certificates).

Any CA who includes authorizations in a certificate, including any conveyed or implied by the subject's DN, shall document in its CPS the mechanisms used to notify the CA of the withdrawal of authorization. Withdrawal of authorization shall result in revocation of the old certificate and, if necessary, the issuance of a new certificate with a different public key and the appropriate authorizations.

Public key certificates shall be issued by the CA to an individual whenever possible. For those cases where there must be several persons acting in one role or in a group, a certificate may be issued by the CA with a Distinguished Name that identifies the group or role. Alternatives for issuing group or role certificates are listed below in order of preference (less secure options shall only be used if more secure options are not feasible).

- unique signature and encryption keys and associated certificates containing the group or role name shall be issued to components acting on behalf of or mediating for a group or role (e.g., mail list agents).
- each individual acting in the same role shall have a separate private signature key and a certificate indicating the role. The individuals acting in the same role or group may share the same encryption certificate and associated private key.
- a signature certificate containing a distinguished name that indicates the role may be issued, and the associated signature private key may be shared by persons acting in that role. (Note that the lack of technically-enforced individual accountability and reliance on procedural mechanisms as described in the requirements below represents a greater security risk to the systems and data protected using these certificates, and must thus be limited to the maximum extent possible. As non-repudiation can no longer be proven, these certificates shall not assert non-repudiation bit in the key usage extension.)

When using role/group certificates, CC/S/As shall establish entities to approve creation of group or role certificates (i.e., RBAAs). These entities in turn shall approve creation of groups and roles and their PKI Sponsors. The role/group PKI Sponsor shall approve members of the groups and roles:

- the group/role PKI Sponsor shall be responsible for ensuring control of the private key and tracking who possesses the private key at all times, including maintaining an ongoing list of Subscribers who have access to use of the private key and also listing, which Subscriber had control of the key at what time. The group/role PKI Sponsor shall forward an initial list and periodically forward all updates since the last submission of this list to the local Security Auditor (i.e., the local ISSO).
- the ISSO is responsible for reviewing the PKI Sponsor's list with an eye towards identification of anomalies.
- a list of those holding the shared private key shall be made available to the CA and RA, upon request.

The procedures for issuing tokens for use in any shared key applications for role/group certificates shall comply with all other stipulations of this policy (e.g., key generation, private key protection, Subscriber obligations). All individuals designated for role/group certificates are required to complete identity authentication in accordance with Section 3.2.3.1.

3.2.6 Criteria for Interoperation

The DoD PKI PMA determines the interoperability criteria for external PKI for interoperation with the PKIs operating under this CP.

The US Federal Public Key Infrastructure (FPKI) Certificate and CRL Profile, FPKI Directory Interoperability Profile, and DoD X.509 CP shall form a basis for assessing interoperability with the DoD PKI. However, the decision to cross certify with an external PKI shall reside with the DoD PKI PMA as specified in Section 1 of this CP.

The DoD PKI operates as an entity of the Federal Bridge Certification Authority (FBCA) (based on Memorandum of Agreement between the DoD PKI PMA with the FPKI Policy Authority).

The *id-fpki-common-derived-pivAuth* OID meets all of the requirements for DoD Medium Software. The *id-fpki-common-derived-pivAuth-hardware* OID meets all of the requirements for DoD Medium Hardware.

Interoperability may also be achieved through trust lists. These trust lists are approved by the DoD PKI PMA.

Interoperability with CAs that issue certificates under different policies that assert different Certificate Policy OIDs may be achieved through policy mapping and cross-certification. All requirements identified in this CP shall be considered as part of any cross-certification decision.

External PKIs that do not demonstrate comparability to the requirements identified in this CP for at least Medium Assurance shall not be cross-certified. Any discrepancies between the operations of a cross certified CA and the requirements identified in this CP shall be documented in a Memorandum of Agreement and are subject to the DoD PKI wavier approval process.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

Re-keying a certificate is the process of issuing a new certificate, identical to a previous certificate but with a new (and different) public key. The new certificate has (corresponding to a new, different private key) a different serial number and may be assigned a different validity period.

An existing certificate may be used for reissuing a new certificate if the current certificate remains valid and the period of identity proofing has not exceeded the maximum in-person identity proofing period established in Section 3.2.3.1.

Practice Note: The longer and more often a key is used, the more susceptible it is to loss or discovery. This weakens the assurance provided to a Relying Party that the unique binding between a key and its named Subscriber is valid. Therefore, it is important that a Subscriber periodically obtains new keys and re-establishes their (or the PKI Sponsor's) identity.

3.3.1 Identification and Authentication for Routine Re-Key

Subscriber certificates may be rekeyed on the basis of existing Subscriber certificates as long as:

- the validity period of the new certificate would not exceed the maximum time period between face-to-face authentications as identified in Table 3-1;
- the maximum life of the new certificate shall not exceed 3 years;
- the assurance level of the new certificate is the same or less than the certificate used to authenticate the request; and,
- all other Subscriber information remains valid.

If the above is not true, the Subscriber must meet the initial identity validation requirements listed in Section 3.2.3.1.

Re-key requests for certificates can be authenticated on the basis of current valid Subscriber certificates as long as the validity period of the new certificate does not extend beyond the periodic in-person authentication requirements listed in the Table 3-1.

CA identity shall be validated through use of the current signature key or initial registration process.

3.3.2 Identification and Authentication for Re-Key After Revocation

Re-key after revocation for all assurance levels shall be done using initial identity validation in accordance with Section 3.2.3.1.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

Revocation requests must be authenticated (see Section 4.9.3). Requests to revoke a certificate may be authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised.

3.5 IDENTIFICATION AND AUTHENTICATION FOR KEY RECOVERY REQUESTS

3.5.1 Subscriber Key Recovery Requests

Subscribers may request the recovery of their own escrowed keys.

For automated self-recovery of private keys, the CA shall authenticate the Subscriber using a valid DoD PKI certificate at the same or higher strength policy OID as the policy OID in the certificate associated with the escrowed key.

Alternatively, the Subscriber may establish his or her identity to an RA, either through the use of a valid DoD PKI certificate at the same or higher strength policy OID as the policy OID in the certificate associated with the escrowed key, or by using the procedures specified in Section 3.2.3.1 for authenticating identity.

If the authentication is not based on digital signatures that can be verified using public key certificates, the RA or TA shall personally verify the identity of the Subscriber prior to initiating the key recovery request.

3.5.2 Third Party Key Recovery Requests

Entities other than the Subscribers (third parties) may request recovery of escrowed keys.

All third-party recovery requests shall be coordinated through an RA or TA, who shall validate the authorization of the requestor in consultation with organization management and/or legal counsel, as appropriate.

The requestor shall establish his or her identity to the RA or TA, either through the use of a valid DoD PKI certificate at the same or higher strength policy OID as the policy OID in the certificate associated with the escrowed key, or by using the procedures specified in Section 3.2.3.1 for authenticating identity.

If the authentication is not based on digital signatures that can be verified using public key certificates, the RA or TA shall personally verify the identity and authority of the requestor prior to initiating the key recovery request.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

All communications among CMAs supporting all certificate life-cycle operations processes shall be authenticated and protected from modification using mechanisms commensurate with the requirements of the data to be protected by the certificates being issued (i.e., communications supporting the issuance of Medium Assurance certificates shall be protected using Medium Assurance certificates, or some other mechanism of equivalent strength). Any electronic transmission of shared secrets shall be protected (e.g., encrypted) using means commensurate with the requirements of the data to be protected by the certificates being issued.

4.1 CERTIFICATE APPLICATION

The applicability statements in this policy shall be considered minimum requirements necessary to support trust in DoD PKI, and to minimize imposition of specific implementation requirements on CAs, RAs, Subscribers, and Relying Parties.

The certificate application process shall provide sufficient information in order to:

- establish the applicant's authorization to request a certificate;
- establish the record of identity of the applicant;
- obtain an applicant's public key and proof of possession of the associated private key; and,
- verify the information included in the certificate.

See Section 3.2 for validation of authorization, establishing identity, and proof of possession.

The certificate application steps may be performed in any order that is convenient for the CMA and Subscribers, and that does not defeat security; but all must be completed prior to certificate enablement.

CAs implementing this CP shall issue certificates to other CAs (including cross-certificates) only as authorized by the DoD PKI PMA and CAs shall only do so within the constraints imposed by the DoD PKI PMA or its designated representatives. Internal NPE CAs shall not issue certificates outside the DoD (or outside the internal environment for which they are specifically authorized).

Requests for CA certificates to be issued from a DoD Root CA shall be submitted to the DoD PKI PMA using the contact provided in Section 1.5.

Prior to issuing a CA certificate from an Internal NPE CA to a new subject CA, the issuing organization shall inform the contact in Section 1.5.1 of the subject CA name.

Certificate application practices and process shall be described in an associated CPSs written to the format of [RFC 3647]. The DoD PKI PMA shall evaluate the submitted CPS for acceptability. The DoD PKI PMA may require an initial compliance audit, performed by parties of the DoD PKI PMA's choosing, to ensure that the CA/RA is prepared to implement all aspects of the submitted CPS prior to the DoD PKI PMA authorizing the CMA to issue and approve certificates asserting one or more of the DoD Policy OIDs listed in Section 1.2 of this CP.

4.1.1 Who Can Submit a Certificate Application

Certificate application may be submitted to the CA by the Subscriber, or an RA on behalf of the Subscriber.

4.1.2 Enrollment Process and Responsibilities

Upon receiving the request, the CA, RA, or TA will:

- verify the identity of the requestor; and,
- verify the authority of the requestor and the integrity of the information in the certificate request.

While the Subscriber may perform the data entry during enrollment, it is still the responsibility of the CMA to verify that the information is correct and accurate. CMAs shall verify all authorization and other attribute information received from an applicant. Information regarding attributes shall be verified via those offices or

roles that have authority to assign the information or attribute. Relationships with these offices or roles shall be established prior to commencement of CA duties and shall be described in a CPS.

4.2 CERTIFICATE APPLICATION PROCESS

It is the responsibility of the CA and RA to verify that the information in certificate applications is accurate. Their CPSs shall specify procedures to verify information in certificate applications.

4.2.1 Performing Identification and Authentication Functions

The identification and authentication of the Subscriber shall be done by the CA, RA, or a TA on behalf of these parties.

4.2.2 Approval or Rejection of Certificate Applications

The certificate application may be rejected for various reasons such as inaccurate information or lack of mission need to provide a certificate to the Subscriber. The CA, RA, or TA may reject a certificate application. The CA, RA, or TA shall work with the appropriate parties to resolve the problem.

A certificate application shall not be considered approved until the CA has accepted the application and decided to issue a certificate.

4.2.3 Time to Process Certificate Applications

See Section 3.2.3.1.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions During Certificate Issuance

The CA shall authenticate a certificate request, ensure that the public key is bound to the correct Subscriber, obtain a proof of possession of the private key, then generate a certificate, and provide the certificate to the Subscriber. The CA shall publish the certificate to a repository in accordance with Section 4.4.2.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The Subscriber shall be notified of certificate issuance.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct Constituting Certificate Acceptance

The Subscriber signature on a certificate acceptance and acknowledgment of responsibilities form (e.g., DD Form 2842) shall constitute acceptance of the certificate. The Subscriber signature shall be collected before a CA allows a Subscriber to make effective use of its private key.

If conducted electronically, the Subscriber's or PKI Sponsor's failure to object to acceptance of the certificate or its contents when obtaining a new certificate shall constitute acceptance of the certificate.

4.4.2 Publication of the Certificate by the CA

CA certificates and Subscriber encryption certificates shall be published to the appropriate repositories.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Cross-certified parties shall be notified upon issuance of new cross-certificates.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

The Subscriber shall not use the signature private key after the associated certificate has been revoked or has expired.

The Subscriber may continue to use the private key solely to decrypt previously encrypted information after the associated certificate has been revoked or has expired.

The Subscriber shall use the private key for DoD-related business only. The use of the private key shall be further limited in accordance with the key usage extension in the certificate.

If the extended key usage extension is present and implies any limitation on the use of the private key, those constraints shall also be observed. For example, the OCSP Responder private key shall be used only for signing OCSP responses.

4.5.2 Relying Party Public Key and Certificate Usage

The Relying Parties shall ensure that a public key in a certificate is used only for the purposes indicated by the key usage extension, if the extension is present.

If the extended key usage extension is present and implies any limitation on the use of the certificate, those constraints shall also be followed.

The Relying Parties shall ensure that a public key in a certificate is used only for the purposes indicated by the certificate policies the certification path is valid for. If the certification path is not valid for any policy (e.g., certificate policies extension is absent in a certificate in the certification path or there is no certificate policy OID common to all the certificates in the certification path after considering policy mapping), the Relying Party shall reject the certificate.

4.6 CERTIFICATE RENEWAL

Renewing a certificate means creating a new certificate with the same name, key, and authorizations as the old one, but with a new validity period and new serial number. The old certificate need not be revoked, but it shall not be further re-keyed, renewed, or updated.

4.6.1 Circumstance for Certificate Renewal

A certificate may be renewed if all of the following are true:

- total key validity lifetime for the public key (including the new certificate and any previous renewals or modifications to the certificate) does not exceed the key validity lifetimes; and,
- the certificate has not reached the end of its validity period; and,
- the certificate has not been revoked; and,
- the in-person identity proofing of the Subscriber (or PKI Sponsor) is current and will not elapse prior to expiration of the new certificate; and,
- the subject name and attributes are still correct.

4.6.2 Who May Request Renewal

The Subscriber (including NPE, CAs, RAs, and OCSP Responders), may request the renewal of their own certificate. The RA may request re-key of a Subscriber's certificate on behalf of the Subscriber. A PKI Sponsor may request renewal of NPE or role/group certificates for which they are responsible.

4.6.3 Processing Certificate Renewal Requests

For manual renewal requests, the renewal process shall follow the initial certificate issuance process described in Sections 3.2.3.1 and 4.3.

For electronic renewal requests, the renewal process shall conduct electronically-authenticated request from the Subscriber as per Section 3.2.3.2. Automated certificate renewal may be conducted by the CA.

4.6.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

See Section 4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

See Section 4.4.2.

4.6.7 Notification of Certificate Issuance by the CA to other Entities

See Section 4.4.3.

4.7 CERTIFICATE RE-KEY

Re-keying a certificate means creating a new certificate with the same name and authorizations as the old one, but with a new key, new validity period and new serial number. After certificate rekey, the old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.7.1 Circumstance for Certificate Re-Key

A certificate shall be re-keyed when it can no longer be renewed as described in Section 4.6.1.

A revoked certificate shall not be re-keyed.

Requirements for CA re-key are described in Section 5.6.

4.7.2 Who May Request Certification of a New Public Key

The Subscriber (including NPE, CAs, RAs, and OCSP Responders) may request the re-key of a of their own certificate. The RA may request re-key of a Subscriber's certificate on behalf of the Subscriber. A PKI Sponsor may request a re-public key on behalf of NPE or role/group certificates for which they are responsible.

4.7.3 Processing Certificate Re-Keying Requests

For manual re-key requests, the re-key process shall follow the initial certificate issuance process described in Sections 3.2.3.1 and 4.3.

For electronic re-key requests, the re-key process shall conduct electronically-authenticated request from the Subscriber as per Section 3.2.3.2. Automated certificate re-key may be conducted by the CA.

4.7.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

See Section 4.4.1.

4.7.6 Publication of the Re-Keyed Certificate by the CA

See Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.8 CERTIFICATE MODIFICATION

Modifying (updating) a certificate means creating a new certificate that has the same or a different key, a different serial number, and differs in one or more other fields, from the old certificate. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

If one or more of the circumstances in Section 4.9.1 apply, then the old certificate shall be revoked.

The CA shall authenticate the validity of any authorizations using the same means as for the initial authorization or means of equal or greater security and assurance.

4.8.1 Circumstance for Certificate Modification

A certificate may be modified if some of the information other than the DN, such as the e-mail address or authorizations, has changed.

If the Subscriber name has changed, the Subscriber shall undergo the initial certificate issuance process.

4.8.2 Who May Request Certificate Modification

The Subscriber (including NPEs, CAs, OCSP Responders, and RAa) may request the modification of their own certificate. The CA or RA may request modification of a Subscriber's certificate on behalf of the Subscriber. A PKI Sponsor may request modification on behalf of NPE or role/group certificates for which they are responsible.

Any change in authorizations shall be validated by the CA, or RA.

4.8.3 Processing Certificate Modification Requests

For manual certificate modification requests, the request process shall follow the initial certificate issuance process described in Sections 3.2.3.1 and 4.3.

For electronic certificate modification requests, the request shall conduct electronic authentication as per Section 3.2.3.2.

Certificates may be automatically modified by the CA.

Changes in authorizations shall be validated by the CA or RA.

4.8.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

See Section 4.4.1.

4.8.6 Publication of the Modified Certificate by the CA

See Section 4.4.2.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 Circumstances for Revocation

A certificate shall be revoked when the binding between the subject and the subject's public key defined within a certificate is no longer considered valid. The following circumstances invalidate the binding and therefore the associated certificate shall be revoked (and place on the CRL):

- identifying information or affiliation components of any names in the certificate become invalid;
- RA or TA negligence conduct (e.g., improperly conducting identity proofing of the Subscriber);
- privilege attributes asserted in the Subscriber's certificate are reduced;
- the Subscriber can be shown to have violated the stipulations of its Subscriber agreement;
- the private key is suspected of compromise; and/or,

- the Subscriber or other authorized party (as defined in the CMA's CPS) asks for his/her certificate to be revoked.

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

Revoked certificates shall be included on all new publications of the CRL until the certificates expire.

Where Subscribers use hardware tokens, revocation is optional if all of the following conditions are met:

- the revocation request was not for key compromise;
- the cryptographic module does not permit the user to export the signature private key;
- the Subscriber surrendered the token to the PKI;
- the token was zeroized or destroyed promptly upon surrender;
- the token has been protected from malicious use between surrender and zeroization or destruction; and,
- an audit record of token surrender, protection, and zeroization is maintained.

4.9.2 Who Can Request a Revocation

A Subscriber may always request revocation of their own certificate. The RA may request the revocation of a Subscriber's certificate on behalf of any authorized party as specified in its CPS. A PKI Sponsor may request revocation of an NPE or role/group certificate for which they are responsible.

Within the PKI, a CMA may revoke certificates without prior notice. Subsequent notification may be provided to the Subscriber or PKI Sponsor in the circumstance of revocation.

4.9.3 Procedure for Revocation Request

Upon receipt of a revocation request from the Subscriber or another authorized party, the CA or RA shall authenticate the revocation request. The CMA may, at its discretion, take reasonable measures to verify the need for revocation. If the revocation request appears to be valid, the CMA shall revoke the certificate.

Except for Internal NPE certificates, any format that is used to request a revocation shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed). The CA may act on a properly authenticated revocation request without involvement of any individual if the request is:

- received from an authorized, authoritative data source;
- authenticated using a certificate issued to the same Subscriber at the same or higher assurance level; or,
- authenticated by a specific CMA authorized individual.

All other requests shall be authenticated by an RA. RAs shall take measures to verify the authority of the requestor and the need for revocation. In general, the RA may, at his or her discretion, take reasonable measures to verify the need for revocation. If the revocation request appears to be valid, the RA shall approve the revocation of the certificate.

Practice Note: A CMA action is required for revocation. Authentication of certificate revocation requests is important to prevent malicious revocation of certificates by unauthorized parties.

An Internal NPE CA may revoke a certificate based on an authenticated revocation request received directly from the Subscriber or an authorized administrator for the local network without the need for another CMA action to approve the revocation request.

For revocation requests executed by the CA based on an authenticated request from an authoritative data source, the CA shall ensure that:

- the CA verifies the integrity and source of the data at a level commensurate with the certificate or certificates being revoked;
- the process implements an independent time-based limit on the number of revocation requests to be executed; and,
- the data source and associated information sent to the CA shall be protected from unauthorized modification to a level commensurate with the level of assurance specified for the certificates to be revoked.

If the revocation is being requested for the reason of key compromise or suspected fraudulent use, then the Subscriber's and the RA's revocation request must so indicate. If a RA performs this on behalf of a Subscriber, the RA shall notify the CA.

4.9.4 Revocation Request Grace Period

There is no grace period for revocation under this policy; Subscribers and authorized PKI entities shall request the revocation of a certificate as soon as the need for revocation comes to their attention.

4.9.5 Time Within Which CA Must Process the Revocation Request

The CA shall process all revocation requests within one hour of receipt. CRL issuance frequency is addressed in Section 4.9.7.

4.9.6 Revocation Checking Requirements for Relying Parties

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

4.9.7 CRL Issuance Frequency

CRLs are periodically issued and posted to a repository, even if there are no changes or updates to be made, to ensure timeliness of information. CRLs may be issued more frequently than required; if there are circumstances under which a CA will post early updates, these shall be spelled out in its CPS. CAs shall ensure that superseded CRLs are removed from the repository upon posting of the latest CRL.

Any CRLs that were generated as the result of a key compromise shall be published expeditiously.

The DoD CAs shall conform to the CRL issuance frequency described in Table 4-1.

CA	Normal CRL Issuance Periodicity	Maximum CRL Issuance Latency for the Reason of Key or CA Compromise
Medium Assurance Offline CAs	At least once every 28 days	Within 6 hours of notification
Internal NPE Offline CAs	At least once every 90 days	Within 18 hours of notification
Online CAs	At least once each day	Within 18 hours of notification

Table 4-1

CAs shall make public a description of how to obtain revocation information for the certificates they publish, and an explanation of the consequences of using dated revocation information. This information shall be given to Subscribers during certificate request or issuance and shall be readily available to any potential Relying Party.

In the case of any DoD PKI CA revocation the DoD PKI PMA shall notify all cross certified external PKIs within the constraints of Table 4-1 above.

4.9.8 Maximum Latency for CRLs

The CRL shall be posted upon generation, but within no more than four hours after generation. A new CRL shall be published no later than the time specified in the nextUpdate field of the most recently published CRL for the same CRL Scope.

4.9.9 On-Line Revocation/Status Checking Availability

CAs and Relying Party client software may optionally support on-line status checking. Since the DoD operates in some environments that cannot accommodate on-line communications, all CAs shall be required to support CRLs. Client software using on-line revocation checking need not obtain or process CRLs.

OCSP Responders shall function in a manner that ensures that:

- accurate and up-to-date information from the authorized CA is used to provide the revocation status that meet or exceed the requirements identified in Section 4.9.7; and,
- revocation status responses provide authentication and integrity services commensurate with the security strength specified as acceptable in Table 4 of [SP 800-57].

4.9.10 On-Line Revocation Checking Requirements

Relying Parties may optionally use on-line status checking.

All CAs shall be required to support CRLs. Client software using on-line revocation checking need not obtain or process CRLs.

DoD relying parties (including CMAs) shall only rely upon OCSP Responders approved in accordance with the requirements of Section 9.6.5.

4.9.11 Other Forms of Revocation Advertisements Available

A CA may also use methods in addition to OCSP Responders and issuing CRLs to publicize the certificates it has revoked. Any alternative method shall meet the following requirements:

- the alternative method shall be described in the CA's approved CPS;
- the alternative method shall provide authentication and integrity services commensurate with Section 6.1.5; and,
- the alternative method shall meet the issuance and latency requirements for CRLs stated in Sections 4.9.7 and 4.9.8.

4.9.12 Special Requirements Related to Key Compromise

A CMA using reason codes must have the ability to transition any reason code to compromise. Stipulations for CRL issuance due to key compromise are provided in Section 4.9.7.

4.9.13 Circumstances for Suspension and Restoration

CAs may support certificate suspension and restoration.

Certificate suspension occurs by marking the certificate as revoked with a reason code of "On Hold." These certificates shall be placed on the next CRL and shall remain on the CRL until the certificates are restored or the certificates expires.

A certificate is restored when the RA reinstates it.

Certificates that are marked as revoked with a reason code other than "On Hold" shall not be restored. The CA shall provide technical mechanisms to enforce this requirement.

4.9.13.1 Circumstances for Suspension

For CAs that support suspension, a certificate shall be suspended when there is reason to believe that the binding between the subject and the subject's public key defined within a certificate is not currently valid, or there may be reason to question the security of the private key, but additional research is necessary to fully determine the status.

Suspension requests may be made for other purposes.

4.9.13.2 Circumstances for Restoration

For CAs that support restoration, a suspended certificate may be restored when the binding between the subject and the subject's public key defined within a certificate is determined to still be valid and the question of the security of the private key is resolved and there was no compromise of the private key.

4.9.14 Who Can Request Suspension and Restoration

4.9.14.1 Who Can Request Suspension

The Subscriber (including NPE, CAs, RAs, and OCSP Responders) may request the suspension of their own certificate. The RA may request suspension of a Subscriber's certificate on behalf of the Subscriber. A PKI Sponsor may only request suspension of certificates for which they are responsible.

Any member of the Subscriber's or PKI Sponsor's chain of command (including organizational security) may request suspension of certificates.

4.9.14.2 Who Can Request Restoration

The requestor of the Suspension may request restoration. The Subscriber may only request restoration if they were the one who requested suspension. Any member of the Subscriber's or PKI Sponsor's chain of command (including organizational security) may request restoration of certificates. A PKI Sponsor may only request restoration of certificates for which they are responsible and if they are the ones who requested the suspension.

4.9.15 Procedure for Suspension and Restoration Requests

4.9.15.1 Procedure for Suspension Request

Any format that is used to request a suspension shall identify the certificate to be suspended, explain the reason for suspension, include an estimated time for the resolution of the suspension, and allow the request to be authenticated (e.g., digitally or manually signed). Digital authentication shall use a certificate at the same or higher assurance level as the certificate to be suspended.

Prior to approving a certificate suspension, the RA shall verify the suspension request, to include authenticating the identity of the requestor and verifying the requestor's authority to request suspension and the validity of the reason for the suspension request.

Once approved by the RA, the CA shall:

- mark the certificate as suspended; and,
- place the certificate on a CRL.

4.9.15.2 Procedure for Restoration Request

Any format that is used to request a restoration shall identify the certificate to be restored, explain the reason for restoration, and allow the request to be authenticated (e.g., digitally or manually signed) at a level commensurate with the certificate being restored. The RA shall validate all restoration requests to ensure that they have appropriate justification and were requested by an authorized entity to prevent malicious restoration of compromised certificates by unauthorized parties.

The private key associated with any suspended certificate shall not be used to authenticate the identity of the restoration requestor.

4.9.16 Limits on Suspension Period

Suspended certificates shall be periodically reviewed to determine if the reason for suspension remains valid. The RA that approved a suspension request shall review suspended certificates monthly or at the time specified in the suspension request, whichever is shorter. The RA shall then revoke any certificate where the suspension has exceeded the original requested suspension period and for which the requestor has not submitted an extension request following the same procedures as the initial request.

4.10 CERTIFICATE STATUS SERVICES

The DoD PKI does not support Certificate Status Authorities such as Simple Certificate Validation Protocol (SCVP).

4.10.1 Operational Characteristics

Not applicable. The DoD PKI does not use Certificate Status Authorities such as SCVP.

4.10.2 Service Availability

Not applicable. The DoD PKI does not use Certificate Status Authorities such as SCVP.

4.10.3 Optional Features

Not applicable. The DoD PKI does not use Certificate Status Authorities such as SCVP.

4.11 END OF SUBSCRIPTION

Subscription is synonymous with the certificate validity period. The subscription ends when the certificate is revoked or expires.

4.12 KEY ESCROW AND RECOVERY

The DoD PKI supports key escrow and recovery for private keys associated with encryption certificates. The DoD PKI does not support key recovery using key encapsulation techniques.

All communications between the key recovery participants shall be secured from disclosure, modification, replay, and substitution. The strength of all cryptographic protocols shall be equal to or greater than that of the keys they protect. Keys shall be protected against disclosure to any party except the authorized requestor. Private keys being escrowed and recovered shall be protected during transmission in accordance with Section 6.2.6.

The cryptography used during storage shall be commensurate with the keys being escrowed.

4.12.1 Key Escrow

4.12.1.1 Circumstances for Key Escrow

Section 6.2.3 specifies the types of certificates that are allowed to be escrowed.

4.12.1.2 Escrowing Keys

Escrowed keys shall be stored in a protected KES that is a component of the CA. All requirements for storage and transfer of private keys shall apply to the process of escrowing private keys.

Escrowed keys shall be maintained within the KES for a minimum of one year after the expiration of the certificate associated with the key. If the certificate associated with the key is renewed or modified without changing the key, the escrowed key shall be maintained within the KES for a minimum of one year after the expiration date of the renewed or modified certificate associated with the key.

4.12.1.3 Notification of Key Escrow to Subscriber

As part of the key escrow process, all Subscribers whose PKI are escrowed shall be notified that the private keys associated with their encryption certificates are being escrowed.

4.12.2 Key Recovery

The DoD PKI supports key escrow and recovery.

When a Subscriber (individual and/or PKI Sponsor or members of a role/group) is issued a new certificate. recovery of private keys associated with previously held encryption certificates may be performed as part of any certificate issuance process to ensure that earlier encryption private keys are available to Subscribers.

During delivery, recovered keys shall be protected against disclosure to any party except the requestor and the Trusted Toles responsible for the recovery.

4.12.2.1 Circumstances for Key Recovery

Escrowed keys may be recovered to support the recovery of encrypted data for business, law enforcement or other requirements. In general, escrowed keys are recovered for the following purposes:

- the original copy of the escrowed key has been lost or damaged and the Subscriber cannot access data encrypted with the corresponding public key;
- the certificate is to be re-keyed and the earlier issued private keys are recovered to be included on the token containing the re-keyed certificate; or,
- an authorized third party requires access to data encrypted with the corresponding public key.

4.12.2.2 Who May Request Key Recovery

Subscribers may request recovery of their own escrowed keys either through an RA or via an automated process directly interfacing with the CA.

RAs may request recovery of escrowed keys on behalf of the Subscriber as part of the re-key or re-issuance process.

Key recovery may also be requested by authorized third parties.

4.12.2.3 Processing Key Recovery Requests

Subscribers may electronically submit requests on their own behalf directly to an RA. Such requests shall be signed by a private key associated with the Subscriber's DoD PKI issued Identity or Signature certificate asserting the same or stronger policy OID as that of the certificate associated with the escrowed key.

Subscribers may manually request recovery of their own escrowed keys from an RA. The Subscriber shall submit a signed request, to either an RA or TA. The RA or TA shall validate the identity of the requestor and forward the request on behalf of the Subscriber via a digitally signed mechanism to an RA authorized to perform key recovery (hereafter referred to as "authorized RA" for key recovery purposes in this Section). The authorized RA shall verify the information in the request.

Subscribers may electronically request recovery of escrowed keys from the CA if they possess a valid DoD PKI issued Identity or Signature certificate asserting the same or stronger policy OID as that of the certificate associated with the escrowed key. The CA shall only provide escrowed keys to Subscribers via an automated means after performing all of the following:

- verifies that the authenticated identity of the requestor is the same as the Subscriber associated with the escrowed keys being requested;
- ensures that the escrowed keys are being sent only to the authenticated Subscriber associated with the escrowed keys; and,
- ensures that the recovered keys are encrypted during transmission in accordance with Section 6.2.6 and that activation data used to protect access to the recovered keys is in accordance with Section 6.4.1.

PKI Sponsors requesting recovery of escrowed keys for which they are responsible shall follow the same process as used for Subscribers.

Third party requestors shall submit requests to either an RA or a TA. Any paper requests shall be hand-signed. Electronic requests shall be digitally signed by a private key associated with a valid DoD PKI issued Identity or Signature certificate asserting the same or stronger policy OID. The RA or TA shall validate the identity of the requestor. An RA shall determine the authority of the requestor to recover the escrowed key in consultation with organization management and/or legal counsel, as appropriate.

RAs or TAs shall forward information via a digitally signed and encrypted email to the authorized RAs performing the manual key recovery.

All manual key recovery operations shall be performed under the control of two authorized RAs throughout all key recovery and delivery processes.

Once the authorized RA has received and validated a key recovery request, the RA shall perform the key recovery with a second authorized RA. The RAs shall authenticate to the CA using a mechanism commensurate with the cryptographic strength of the strongest key stored requested.

All copies of recovered keys shall be continuously protected using mechanisms at least commensurate with the level of the data the key provides access to or protects by the recovering Trusted Roles during the recovery and delivery to the authenticated and authorized requestor. Recovered keys shall be protected during transmission in accordance with Section 6.2.6 and activation data used to protect access to the recovered keys shall be in accordance with Section 6.4.1.

4.12.2.4 Notification of Key Recovery to Subscriber

Subscribers may be notified of requests using the Subscriber's private key.

There is no requirement to notify the Subscriber of key recovery requests made by parties other than the Subscriber.

4.12.2.5 Notification of Key Recovery by the CA to Other Entities

There is no requirement to notify other entities of key recovery requests.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

All CMA equipment, including cryptographic modules, shall be protected from theft, loss, and unauthorized access at all times. Unauthorized use of CMA equipment is forbidden. Physical security controls shall be implemented that protect the CMA hardware and software from unauthorized use.

CAs, CMSs, and OCSP Responders shall consist of equipment dedicated to their CMA functions. They shall not perform non-CMA related functions.

All the physical control requirements specified below apply equally to all CMAs, and any remote workstations used to administer the CMAs except where specifically noted.

5.1.1 Site Location and Construction

The location and construction of the facility that will house CMA equipment and operations shall be in accordance with DoD and local policy for protecting information of the same value or classification as the material that will be protected by the public key certificates issued or managed there.

5.1.2 Physical Access

Internal NPE CAs and cryptographic modules shall be provided with physical security controls equivalent to those provided to other high value assets (e.g., domain controllers) on the network.

All other CA and OCSP Responder equipment and cryptographic modules shall always:

- be protected from unauthorized access;
- ensure that all removable media and paper containing sensitive plain-text information is stored in secure containers;
- be manually or electronically monitored for unauthorized intrusion at all times;
- ensure an access log is maintained and inspected periodically; and,
- require the presence of at least two Trusted Role personnel (see Section 5.2.1) for any access to the CA or the OCSP Responder equipment or to the CA or the OCSP Responder cryptographic module.

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

When not in use, removable CA and OCSP Responder cryptographic modules, and any activation information used to access or enable the cryptographic modules or equipment, shall be placed in locked containers sufficient for housing equipment and information commensurate with the classification, sensitivity, or value of the information being protected by the certificates issued by the CA. Activation data shall either be memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module.

For other than Internal NPE CAs, a security check of the facility housing CA and OCSP Responder equipment shall occur prior to leaving the facility unattended. The check shall verify that:

- 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”);
- any security containers are properly secured;
- physical security systems (e.g., door locks, vent covers) are functioning properly; and,
- the area is secured against unauthorized access.

A person or group of persons shall be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance shall be maintained.

If the facility is not continuously attended, procedures shall be put into place to ensure protection of

equipment and records.

Facilities housing CA and OCSP Responder equipment shall, if unattended for periods greater than 24 hours, be protected by an intrusion detection system. Additionally, a check shall be made at least once every 24 hours to ensure that no attempts to defeat the physical security mechanisms have been made.

For Internal NPE operating on the Secret Fabric, any hardware cryptographic module used for issuing certificates whose keys will protect classified information is classified at the level of that information, both when in use and when not in use. When not in use, the cryptographic module shall be stored in a container approved for classified cryptographic storage at the classification level associated with the cryptographic module (at a minimum), where access is allowed only to authorized CMA operators as defined in Section 5.2.

5.1.3 Power and Air Conditioning

The facility, which houses the CA, CSS, and OCSP Responder equipment, shall be supplied with power and air conditioning sufficient to create a reliable operating environment.

The CA, CSS, and OCSP Responder equipment shall have or be provided with sufficient alternate power (e.g., generator power) to execute a standard shutdown (including locking out input, finishing any pending actions, and recording the state of the equipment) before lack of primary power or air conditioning causes the CA, CSS, and OCSP Responder equipment to cease functioning.

Power and air conditioning support to the repository that are the primary source of CA certificates and/or CRLs for access by relying parties shall be sufficient to ensure that availability requirements of Section 2.1 are met.

5.1.4 Water Exposures

CMA equipment shall be installed such that it is not in danger of exposure to water, e.g., on tables or elevated floors. Moisture detectors shall be installed in areas susceptible to flooding. CMAs that have sprinklers for fire control shall have a contingency plan for recovery should the sprinklers cause water damage to the CMA equipment.

5.1.5 Fire Prevention and Protection

CMA equipment shall be installed such that the possibility of fire is minimized. CMA operating material (e.g., software, keys) shall be stored such that they are protected from fire. CMA facilities shall be equipped with heat and smoke detectors, alarms, and a fire suppression system appropriate for computer equipment.

A description of the CMA's approach for recovery from a fire disaster shall be included in the Disaster Recovery Plan required by Section 5.7.4.

5.1.6 Media Storage

Media shall be stored so as to protect it from accidental damage (e.g., water, fire, electromagnetic). Media that contains sensitive information (e.g., identified in Section 9.4, security audit, archive, backup information shall be protected from unauthorized access.

5.1.7 Waste Disposal

Media used to collect or transmit sensitive DoD PKI information (e.g., personal information identified in Section 9.4, security audit, archive, backup information) shall be destroyed, such that the information is unrecoverable, prior to disposal. Destruction of media containing private key material shall comply with the stipulations in Section 6.2.10.

Any classified media or papers shall be destroyed in accordance with the applicable policy for destruction of such material.

5.1.8 Off-Site Backup

CA system backups, sufficient to recover from system failure, shall be made on a periodic schedule.

One full backup of the CAs that are continuously operated (for periods of one week or longer) shall be made at least once a week and shall be stored at an offsite location (separate from the CA).

For intermittently operated CAs, the full system backup shall be made each time the system is turned on or once a week, whichever is less frequent.

The backup shall be stored at a site with physical and procedural controls commensurate with those for the operational CA system.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

Trusted Roles are filled by CMA personnel. A Trusted Role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously.

Three steps shall be taken to select personnel to perform these Trusted Roles:

- ensure that the person filling the role is trustworthy and properly trained;
- assign individuals to only one role; and,
- distribute the functions among several roles so that any malicious activity requires collusion.

5.2.1.1 CMA Trusted Roles

All CMAs shall be supported by personnel filling Trusted Role and specifically identified for those roles. Separation of these roles and responsibilities shall be in accordance with Section 5.2.4.

The primary CMA Trusted Roles include the following:

- *Officer* – authorized to request, approve, or perform certificate issuance, revocation, or key recovery;
- *Security Auditor* – authorized to review, maintain, and archive audit logs; the types of auditors (specifically, these Security Auditors (i.e., ISSO) oversees/reviews security audit logs, performs/oversees archive and deletion functions of security audit logs, performs/oversees internal audits and other archive data as described in Sections 5.4 and 5.5 of this CP;
- *Operator* – authorized to perform system backup and recovery (may be combined with the Administrator role);
- *Administrator* – authorized to install, configure, and maintain the CMA; establish and maintain system accounts; configure audit parameters; conduct system backups and upgrades; generate PKI component keys (Administrators do not issue certificates to Subscribers). Supports the ISSO in the consolidation/collection of audit logs for review and transfer of data to archives. This role includes System Administrators or any persons with the responsibility to perform the above administrative functions impacting CMA equipment.

CMAs are not required to utilize all Trusted Roles in the performance of its functions. If utilized, the CMA shall ensure separation of duties in accordance with Section 5.2.4.

The CMA shall maintain lists, including names, organizations, and contact information, of those who act in Trusted Roles.

5.2.1.2 Other Roles

The CMA (and CC/S/A) may employ other roles to support PKI functions. When employing other roles, a CMA shall define allocated responsibilities that ensure the proper, safe, and secure operation of the CMA equipment and procedures. If additional roles are identified to support implementation, the CMA shall enforce separation of duties among the characteristics of duties performed by the primary Trusted Roles listed in Section 5.2.1.1. Other roles and responsibilities include (but are not limited to) the following:

- *Agents* – individuals authorized to act as representatives of a CMA in performing Subscriber identity validation during the registration process; authorized to deliver a Subscriber's cryptographic module (i.e., Trusted Agent); authorized to act in support of key recovery (i.e., Key Recovery Agent)
- *Authorities* – entities authorized by the CC/S/A to validate group/role Subscriber authorization to act on in a specified role/on behalf of the identified group (i.e., Role Based Attribute Authorities); to verify the association of attributes to an identity for code signing (i.e., Code Base Attribute Authorities);
- *Sponsors* – entities authorized by a CC/S/A to act on behalf of a NPE or Group/Role Subscribers (i.e., PKI Sponsors); PKI Sponsors register NPEs in accordance with Section 3.2.3.3, and are otherwise responsible for meeting the obligations of Subscribers as defined throughout this document; and,
- *Compliance Auditor*s – independent third party responsible for performance of compliance audit in accordance with Section 8 of this CP.

5.2.2 Number of Persons Required for Task

Two-person control shall be enforced while performing the following functions:

- CA and OCSP Responders key generation, key activation and key backup;
- access to CA or OCSP Responder signing keys backed up for disaster recovery;
- certificate requests (including the public key generation and delivery) for the purpose of generating a CA or OCSP certificate; and,
- access to an escrowed private key as part of key recovery and subsequent delivery to a third-party requestor.

Collection of the audit records from the CA system shall be performed by, witnessed by or under the control of two-or-more Trusted Roles who are different from the individuals who, in combination, command the CA signature key.

Where multiparty control is required, all participants shall serve in a Trusted Role on the CMA as defined in Section 5.2.1. Multiparty control shall not be achieved using personnel that serve in the ISSO or Compliance Auditor Trusted Role. The names of the parties used for two-person control shall be maintained on a list that shall be made available for inspection during compliance audits.

Key recovery of escrowed private key shall be performed under two-person control until the key is delivered to the third party.

5.2.3 Identification and Authentication for Each Role

Individuals holding CMA Trusted Roles shall be appointed by an appropriate approving authority. The approval and acceptance by the individual appointed shall be recorded in a secure and auditable fashion.

Person occupying a Trusted Role shall authenticate to a local infrastructure component of the DoD PKI using a valid DoD PKI certificate or other approved authentication method.

Persons occupying a Trusted Role shall authenticate to a remote infrastructure component of the DoD PKI using a valid DoD X.509 certificate.

All Trusted Roles who operate a CMS shall be allowed access only when authenticated using a method commensurate with *id-dod-mediumHardware.*

5.2.4 Roles Requiring Separation of Duties

Under no circumstances shall the incumbent of a CMA role perform its own compliance or Security Auditor function.

A Compliance Auditor shall not perform any other role on the CMA.

A Security Officer (i.e., ISSO) shall not perform any other role on the CMA.

An RA shall not perform system administrator/ISSO duties on any system where they exercise CMA authority.

The applicable CMA CPS shall describe how these role separation requirements are met.

No individual shall have more than one identity on any CMA.

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

Persons shall be selected for any CMA or other Trusted Role on the basis of loyalty to the United States, their trustworthiness, and integrity. CMA personnel may be US uniformed service members, government civilian employees, or designated contractors of any organization authorized by the DoD PKI PMA to possess and issue DoD PKI certificates in accordance this CP.

All personnel holding a CMA Trusted Role shall be US citizens and hold a US security clearance. All personnel filling other roles shall hold an active US security clearance or be US citizens with a current background investigation.

Personnel assigned to Trusted Roles within the DoD PKI shall:

- have successfully completed an appropriate training program;
- have demonstrated the ability to perform their duties;
- be trustworthy;
- have no other duties that would interfere or conflict with their duties as a CMA;
- have not been previously relieved of CMA or COMSEC custodian 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; and,
- be appointed in writing by an approving authority, or be party to a contract for PKI services.

For Internal NPE, personnel issuing or requesting certificates for classified environments (e.g., Confidential or Secret) shall hold a security clearance equal to or higher than the environment for which they are requesting the certificate.

5.3.2 Background Check Procedures

CMA Trusted Roles shall follow standard DoD security clearance processes.

For other roles, local service, agency, or community procedures shall be followed to determine the type of background check or follow clearance requirements for security clearance.

5.3.3 Training Requirements

A training plan shall be established for a CMA installation, and training completed by the personnel shall be documented.

Topics that shall be included in this training plan include (but is not limited to) the topics found in Table 5-1 for the corresponding roles.

Topic	DoD PKI CA and OCSP Responder Operations Staff	CMS Operational Staff	RA Operations Staff	Security and Compliance Auditors	TA
Requirements of this policy and local procedures	X	X	X	X	X

Topic	DoD PKI CA and OCSP Responder Operations Staff	CMS Operational Staff	RA Operations Staff	Security and Compliance Auditors	TA
PKI duties that they are expected to perform	X	X	X	X	X
CMA security principles and mechanisms	X	X	X	X	
Roles-specific PKI CPSs	X	X	X	X	X
PKI equipment and software versions authorized for use in CMA	X	X	X	X	
Disaster recovery and incident reporting procedures	X	X	X	X	
Changes or updates to PKI policy, practices or governance (See Section 5.3.4)	X	X	X	X	

Table 5-1

5.3.4 Retraining Frequency and Requirements

All personnel filling DoD PKI roles shall be aware of changes in the CMA policies operation, practices, and governance. Any significant change to the CMA requirements, practices, or operation shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are CA software or hardware upgrade, changes in automated security systems, changes to certification or registration practices, updates to CMS operations, or relocation of CA equipment.

Retraining completed by personnel shall be documented.

5.3.5 Job Rotation Frequency and Sequence

This policy makes no stipulation regarding frequency or sequence of job rotation. Local policies, which do impose requirements, shall provide for continuity and integrity of the DoD PKI service.

Job rotation shall not violate role separation. All access rights associated with a previous role shall be terminated. All job rotations shall be documented. Individuals assuming an auditor role shall not audit their own work from a previous role.

5.3.6 Sanctions for Unauthorized Actions

A CMA shall take appropriate administrative and disciplinary actions against personnel who violate this policy, applicable CPS, or other published procedures.

Significant violation of policy may result in revocation of the individual's public key certificate or a formal notification by the DoD PKI PMA to cease PKI related operations.

See Section 5.7.1 for notification regarding incidents concerning violations.

See Section 8.5 for actions taken as a result of deficiency.

See Section 9.13 for any disputes arising from CMA actions.

5.3.7 Independent Contractor Requirements

Contractor filling Trusted Roles on DoD PKI are subject to all requirements stipulated in this CP, applicable CPS, or other published procedures.

PKI vendors who provide services to the DoD shall establish procedures to ensure that any subcontractors perform in accordance with the CP and the applicable CPS.

5.3.8 Documentation Supplied to Personnel

Documentation sufficient to define duties and procedures for each role shall be provided to the personnel filling that role.

5.4 AUDIT LOGGING PROCEDURES

Audit logs files shall be generated for all events related to the security of the CMA as identified in Section 5.4.1. All security audit logs shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in Section 5.4.1 shall be maintained in accordance with Section 5.4.3.

Where possible, security logs shall be collected automatically. Where this is not possible, the use of a logbook (physical or electronic) shall be used.

Security audit logging capabilities of CMA equipment shall be enabled during installation. Audit logs shall implement controls to allow for the detection of attempts to modify or delete entries. This shall 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.

In the case where CMA equipment operates in a virtual machine environment (VME), requirements in this section and subsections apply to both the host[4] and the hypervisor event logs.

5.4.1 Types of Events Recorded

Audit requirements apply to all CMA system (including both VME and hypervisor if applicable).

For each auditable event defined in this section, the CMA security audit record shall include, at a minimum:

- what type of event occurred;
- when (date and time) the event occurred;
- where the event occurred;
- source of the event;
- identity of any individuals, subjects, or objects/entities associated with the event; and,
- success or failure.

At a minimum, the events identified in Table 5-1 shall be recorded by each system or individual that performs the action.

Event Type	Event
Security Audit	• Any changes to the Audit parameters, e.g., audit frequency, type of event audited • Any attempt to delete or modify the Audit logs Audit Log review
Identification and Authentication	• Successful and unsuccessful attempts to assume a role • The value of maximum authentication attempts is changed • The maximum number of unsuccessful authentication attempts occurs during a user login • An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts

[4] The various operating systems executing on a hypervisor are referenced by one or more of the following terms which are considered synonymous in this CP: host, virtual machine, and guest operating system.

Event Type	Event
	• An Administrator changes the type of authenticator, e.g., from password to biometrics
Local Data Entry	• Any security-relevant data that is entered in the system (e.g., account management, directory access, policy or privilege change)
Remote Data Entry	• Any security-relevant messages that are received by the system
Data Export and Output	• Any successful and unsuccessful requests for private, sensitive, classified, or security-relevant information
Key Generation	• Whenever the CA generates a key (not mandatory for single session or one-time use symmetric keys)
Private Key Load and Storage	• The loading of Component private keys • Any access to certificate subject private keys retained within the CA for key recovery purposes
Trusted Public Key Entry, Deletion, and Storage	• Any changes to the trusted public keys, including additions and deletions
Private Key Export	• The export of private keys (keys used for a single session or message are excluded)
Certificate Registration	• Any certificate requests
Certificate Status	• Any certificate revocation, modification, suspension, re-key, or renewal requests
Certificate Status Change Approval	• The approval or rejection of a certificate status change request
CMA configuration	• Any security-relevant changes to the configuration of the CMA • Configuration changes to the CMA systems, including hardware, software, operating system, patches, or security profiles
Account Administration	• Roles and users are added or deleted • The access control privileges of a user account or a role are modified
Certificate Profile Management	• All changes to the certificate profile
Revocation Profile Management	• All changes to the revocation profile
CRL Profile Management	• All changes to the CRL profile
Personnel Controls	• Appointment of an individual to a Trusted Role • Designation of personnel for multiparty control • Training of individuals appointed to the RA role

Event Type	Event
Miscellaneous	• Installation of CMA operating systems and applications • Physically accessing, loading, zeroizing, transferring keys to or from, backing-up, • acquiring, or destroying cryptographic modules • Installing hardware cryptographic modules • Removing hardware cryptographic modules • Receiving, servicing (e.g., keying or other cryptologic manipulations), and shipping hardware cryptographic modules • System startup • Logon attempts to CMA applications • Receipt of hardware / software • Attempts to set passwords • Attempts to modify passwords • Backing up CMA internal databases • Restoring CMA internal databases • File manipulation (e.g., creation, renaming, moving) • Posting of any material to a repository • Access to CMA internal databases • All certificate compromise notification requests • Re-keying any component private keys to include the CA • A message from any source received by any CA requesting an action related to the operational state of the CA • Any requests and actions taken in response to messages requesting CA actions not covered elsewhere • Installation, access, and modification (to include changes in configuration files, security profiles, and administrator privileges) of CMA system • Any use of the CA signing key • Messages received from any source requesting RA actions, (certificate requests, compromise notification, key recovery requests, key recovery approval) • Any actions taken in response to requests for RA actions
Physical Access and Site Security	• Personnel access to room housing CA • Physical access to the CA • Known or suspected violations of physical security • Any known or suspected violations of physical security, suspected or known attempts to attack the CMA equipment via network attacks, equipment failures, power outages, network failures, or violations of this certificate policy
Anomalies	• Software error conditions • Software check integrity failures • Receipt of improper messages • Misrouted messages • Network attacks (suspected or confirmed) • Equipment failure • Electrical power outages • Uninterruptible power supply (UPS) failure • Obvious and significant network service or access failures • Violations of certificate policy • Violations of certification practice statement • Resetting operating system clock • Network failures

Event Type	Event
Key Escrow and Recovery	• Server installation, access, and modification (to include changes in configuration files, security profiles, administrator privileges) • Key escrow database application access (e.g., logon/logoff) • Messages received from any source requesting key escrow database actions, (e.g., escrowed key retrieval requests) • Messages sent to any destination authorizing key recovery actions, (e.g., first party escrowed key retrieval authorizations, second party key recovery approvals) • Actions taken in response to requests for key escrow database actions • Physical access to, loading, zeroizing, transferring keys to or from, backing-up, acquiring or destroying key escrow database cryptographic modules • Receipt of keys for escrow and posting of these keys to the key escrow database • Retrieval, packaging (e.g., keying or other cryptologic manipulations), securing, and shipping copies of escrowed keys • Transfer of escrowed keys to requestors • Any security-relevant actions performed in support of delivery of escrowed keys • Requestor identity and authorization verification (including copies of authorizations; e.g., court orders) supporting key recovery requests

Table 5-2

A CMA shall record the process that was followed for each certificate issued to an individual. At a minimum, process documentation must include:

- the identity of the person performing the identification;
- a signed declaration by the person that verified the identity of the Subscriber as required by this certificate policy;
- the method used to authenticate the individual's identity (including identification type and unique numeric or alphanumeric identifier if appropriate and/or certificate information used for authentication if electronically authenticating);
- a signed declaration from the individual receiving a certificate; and,
- the date of the verification of an individual's identity.

5.4.2 Frequency of Reviewing Audit Logs

For Medium Assurance, CMA log reviews shall be conducted monthly.

All CA and CMS audit logs shall be reviewed.

For monthly RA audit logs, a Security Auditor (i.e., ISSO) may conduct a review of a sampling of logs generated since the last review conducted.

For Internal NPE CAs, audit logs shall be processed and reviewed as often and as thoroughly as the operating organization processes and reviews high-value network asset and application event logs.

5.4.3 Retention Period of Audit Log

All audit logs shall be accessible until reviewed, in addition to the specific records being archived as described in Section 5.5.

All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

For Internal NPE CAs, security audit data shall be retained until the certificate related to the event expires.

5.4.4 Protection of Audit Log

The CMA shall implement procedures to ensure that the security audit data is transferred prior to overwriting or overflow of automated security audit log files.

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

The audit log collection system shall enforce separation of duties and access to logs based on the CMA Trusted Role of an individual.

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

Procedures shall be implemented to protect audit records from deletion before archiving or backup.

For Internal NPE CAs, security audit data shall be protected as other high-value network assets and application event logs.

5.4.5 Audit Log Retention Procedures

See Section 5.4.3 for retention procedures.

See Section 5.5 for archiving procedures.

For Internal NPE CAs, security audit data are not required to be backed up.

5.4.6 Audit Collection System (Internal vs. External)

The audit log collection system may be internal or external to the CMA.

Operating system security audit processes shall be invoked at system startup and cease only at system shutdown.

All application security audit processes shall be invoked at system startup and cease only at application shutdown.

Should it become apparent that an automated security audit system has failed; the CMA shall cease all operation except for revocation processing until the security audit capability can be restored. Under these circumstances, the CMA shall employ mechanisms to preclude unauthorized CMA functions.

5.4.7 Notification to Event-Causing Subject

There is 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

CMAs shall perform routine vulnerability assessments of the security controls described in this CP and as required by [DODI 8500.01] and [DoDI 8510.01].

The ISSO shall conduct and document results of all audit log reviews. A record of this review and any actions taken as a result of subsequent reviews shall be explained in an audit log summary. This review shall be retained as a part of the long-term archive.

The Security Auditor shall verify that:

- the audit logs have not been tampered with;

- events such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses are identified; and,
- continuity of the security audit data is checked.

The CMA operations personnel shall be watchful for attempts to violate the integrity of the CMA, including the equipment, physical location, and personnel.

For Internal NPE CAs, vulnerability assessments shall be performed as are conducted for other high-value network assets and applications.

5.5 RECORDS ARCHIVAL

In the case where CMA equipment operates in a VME, requirements in this section and subsections apply to both the host and the hypervisor event logs.

5.5.1 Types of Records Archived

CMA archive records shall be sufficiently detailed as to verify that the PKI was properly operated as well as verify the status (e.g., valid, revoked, suspended, restored) of any certificate throughout its validity period. At a minimum, the following data shall be archived (as applicable):

- CMA Accreditation (if necessary);
- Certificate Policy;
- CPSs;
- contractual obligations;
- other agreements concerning operations of the CMA;
- system and equipment configurations;
- modifications and updates to system or configuration;
- 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);
- all records related to certificate status changes (e.g., revocation, suspension, or restoration) (whether generated directly on the CA or generated as part of a related external system or process);
- Subscriber identity authentication data (as per Section 3.2.3);
- documentation of receipt and acceptance of certificates;
- Subscriber Agreements;
- documentation of receipt of tokens;
- all certificates issued or published;
- record of CA re-key;
- other data or applications to verify archive contents;
- audit summary reports generated by internal reviews;
- documentation generated during third-party audits;
- any changes to the Audit parameters (e.g., audit frequency, type of event audited);
- any attempts to delete or modify the Audit logs;
- whenever the CA generates a key (not required for single session or one-time use symmetric keys);
- all access to certificate subject private keys retained for key recovery purposes;
- changes to trusted public keys used or published by the CA (including certificates used for trusts between the CA and other components of the CMA);
- export of private and secret keys (not required for single session or one-time use symmetric keys);
- approval or rejection of a certificate status change request;
- record of an individual being added or removed from a Trusted Role (and who added/removed them from that role);
- destruction of cryptographic modules;
- all certificate compromise notifications;
- remedial actions taken as a result of a violation of physical security;
- violations of Certificate Policy;

- violations of a CPS; and,
- escrowed keys.

5.5.2 Retention Period of Archive

Archived retention periods shall begin when a record is generated.

Archive records covered by either a General Records Schedule established by the National Archives and Records Administration or an agency-specific schedule as applicable shall be retained as specified in the approved records schedule in accordance with *DoD Records Management Program* [DoDI 5015.02]. Otherwise, archive records shall be retained in an accessible fashion for the following periods (or longer as may be needed for business requirements, whichever is later):

Assurance Level	Minimum Retention Period
Internal NPE	7 Years, 6 months
All other policies	10 Years, 6 Months

Table 5-3

Applications necessary to read these archives shall be maintained for at least the applicable retention period above.

5.5.3 Protection of Archive

CMA archives shall be under the control of the ISSO.

CMA archives shall not be deleted until the after the end of the archive period.

Archive data may be moved to another medium periodically (e.g., if original media cannot retain the data for the entire required period). Transfer of archive shall be done so as not to invalidate CMA applied signatures.

The CMA shall maintain a list of people authorized to amend or delete the archive and shall make this list available during compliance audits.

CMA archive media shall be stored in a safe and secure storage facility in a manner where there is a low probability of data loss. Archive media shall be stored in a facility with sufficient separation from operational data. Prior to archive, archive records shall be labeled with the CMA's distinguished name, the date range, and the classification.

For Internal NPE CAs, archive data shall be protected as for other high-value network asset and application data.

5.5.4 Archive Retention Procedures

The CMA shall describe archive retention procedures for collection, retention and management in applicable CMA CPS.

5.5.5 Requirements for Time-Stamping of Records

Archived records shall contain information necessary to allow the Security Auditor to determine when an event occurred. Time precision used for the CMA shall be such that the sequence of events can be determined. The CMA shall document in applicable CPS on how they ensure that time stamps are consistent with an authoritative time standard. See Section 6.8.

Physical logs shall capture time and date entry of an event; other manual records only require the date on the document.

5.5.6 Archive Collection System (Internal vs. External)

Archive data may be collected in any expedient manner.

5.5.7 Procedures to Obtain and Verify Archive Information

Procedures detailing how to create, verify, package, transmit, and send archive information shall be captured in applicable CMA CPS or procedures handbook. This shall include practices on how requests and release authorization of archive records (to Subscribers for individual transactions or to authorized third parties) shall be conducted.

5.6 KEY CHANGEOVER

Upon re-key of a CA, only the new private key shall be used to sign certificates.

An old private key of the CA shall continue to be used to sign CRL and OCSP Responder certificates until all certificates signed using that old private key have expired.

A CA private key shall be destroyed when the CA certificate has expired or when the CA public key is no longer valid.

CAs shall not issue certificates that extend beyond the validity period of the CA public keys.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

All CMAs shall have an incident handling process which documents any security incident. Any security incident shall include violations or threats of violations to the system, improper usage, malicious or anomalous activity and violations to this CP or applicable CPS.

Any suspected or confirmed compromised involving a CMA shall be reported to the DoD PKI PMA. DoD PKI PMA shall make additional notifications to the FPKI PA as required by the MOA between the DoD PKI PMA and the FPKI PA. All incidents shall be reported to the DoD PKI PMA including (but are not limited to) the following:

- suspected or detected compromise of any CMA system or subsystem;
- physical or electronic penetration of any CMA system or subsystem;
- successful denial or service attacks on any CMA system or subsystem;
- any incident preventing a DoD PKI CA from issuing and/or publishing a CRL prior to the time; and, indicated in the next *nextUpdate* field in the currently published CRL.

Incident reporting shall include the following data:

- CMA components that were affected by the incident;
- CA interpretation of the incident;
- impact of the incident;
- when the incident was discovered;
- when the incident occurred or may have occurred; and,
- a complete list of all certificates that may have been impacted or are not compliant with this CP/applicable CPS as a result of the incident.

Upon completion of all remediation action, the CMA shall notify the DoD PKI PMA.

If a CA key is suspected of compromise, the procedures outlined in Section 5.7.3 shall be followed. Otherwise, the scope of potential damage shall be assessed in order to determine if the CA needs to be rebuilt, only some certificates need to be revoked, and/or the CA key needs to be declared compromised.

If the CMA or TA is compromised, all certificates issued to the CMA or TA shall be revoked, if applicable. The damage caused by the CMA or TA compromise shall be assessed and all Subscriber certificates that may have been compromised shall be revoked, Subscribers shall be notified of such revocation.

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

If computer resources, software, and/or data corruption occurs, CMAs what take the following actions:

- notify the DoD PKI PMA (See Section 5.7.1);
- determine extent of risk due to operations since the last point of backup;
- ensure the system's integrity has been restored prior to returning to operations; and,
- reestablish operations.

For reestablishing operations when the CA signing keys are not destroyed, the system has been restored, and the risk of reestablishing operations is deemed negligible, priority shall be given to the ability to generate certificate status information within the CRL issuance schedule as specified in Section 4.9.7. Priority shall also be given to generating delegated OCSP Responder certificates before expiration of the current delegated OCSP Responder certificates.

For reestablishing operations, when the CA signing key are destroyed, the integrity of the system cannot be restored, or the risk is deemed substantial, priority shall be given to generation of a new CA signing key pair.

The CA shall maintain backup copies of system, databases, and private keys in order to rebuild the CA capability in case of hardware, software and/or data corruption (see Section 5.1.8).

5.7.3 Entity Private Key Compromise Procedures

5.7.3.1 CA Compromise Procedures

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

- all issuing CAs shall revoke that subject CA's certificate;
- issuing CA shall publish revocation information immediately in the most expedient manner; and,
- issuing CA and subject CA management authorities shall immediately notify the DoD PKI PMA.

Subsequent to these procedures, the CA installation shall establish the CA as described in Section 5.7.4. If the revoked CA is a Root CA, the trusted self-signed certificate of the revoked CA shall be removed from DoD Relying Party application, and a new trusted self-signed certificate shall be distributed via secure out-of-band mechanisms.

5.7.3.2 OCSP Responder Compromise Procedures

In the event of a OCSP Responder key compromise, the following operations shall be performed:

- issuing CA that issued the OCSP Responder certificate shall revoke that certificate issued;
- revocation information shall be published immediately (in the most expedient, authenticated, and trusted manner); and,
- issuing CA management authority shall immediately notify the DoD PKI PMA.

After these actions have been performed, the OCSP Responder shall be re-keyed. Cross-certified PKIs shall be notified of the compromise so that they can notify all Subscribers and other Relying Parties to remove the trust from Relying Party applications and install the re-keyed certificate.

If a CA-Hosted DoD PKI OCSP Responder is suspected or known to be compromised or misused, the event shall be treated as a compromise of the hosting CA.

5.7.3.3 RA Compromise Procedures

In the event of a RA key compromise, the following operations shall be performed:

- the CA that issued the RA's certificate shall revoke that certificate;
- revocation information shall be published immediately in the most expedient manner;
- the compromise shall be investigated to determine the date of actual or potential compromise;
- all certificates approved by the RA since the date of the actual or potential compromise shall be revoked;
- all associated escrowed keys shall be identified for potential exposure and revoked if exposed; and,
- the CA management authority shall immediately notify the DoD PKI PMA.

5.7.4 Business Continuity Capabilities After a Disaster

CAs shall maintain an Authorizing Official- approved Disaster Recovery Plan.

In the case of a disaster in which a CA's equipment is damaged and inoperative, the CA operations shall be reestablished as quickly as possible, giving priority to the ability to revoke Subscriber's certificates.

If the CA cannot reestablish revocation capabilities to meet the requirements of Section 4.9.7, then the CA must report to the DoD PKI PMA. The DoD PKI PMA shall decide whether to declare the CA signing key as compromised. and the DoD PKI PMA may decide to re-key CA keys, all cross-certificates, and all Subscriber certificates, or to allow additional time for reestablishment of the CA's revocation capability.

In the case of a disaster whereby a CA installation is physically damaged and all copies of the CA signature key are destroyed as a result, the CA shall request revocation of its certificates. If the CA is the Root CA, the trusted self-signed certificate shall be removed from the DoD Relying Parties applications. A new CA shall be established if determined to be required by the DoD PKI PMA.

5.8 CA OR RA TERMINATION

5.8.1 CA Termination

In case of cessation of a CA operation, the certificate issued to the CA shall be revoked, unless the certificate has expired. If the CA is a Root CA, the trusted certificate shall be removed from all DoD relying parties in an expeditious manner.

For any CA termination, the responsible management authority shall ensure that all security data are archived and shall maintain possession of all archive records and any audit logs. Prior to CA termination, CAs shall provide archived data to a DoD PKI PMA-approved DoD archival facility.

5.8.2 RA Termination

If a RA is terminated, the RA's certificates shall be revoked. Any privileges assigned to that RA on the CMA systems shall be removed.

Termination of an RA for negligence or cause is treated as a compromise. See Section 4.9.1 and 5.7.1.

5.8.3 TA Termination

If a TA is terminated, the RA shall indicate that the TA is no longer approved as a TA. Any TA certificates issued to the terminated individual shall be revoked.

Termination of an TA for negligence or cause is treated as a compromise. See Section 4.9.1 and 5.7.1.

6 TECHNICAL SECURITY CONTROLS

In this CP, specified [FIPS 140] validation levels are minimums.

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

All keys and intermediate keys and pseudo-random numbers used for all key generation shall be generated using a FIPS-approved method. A private key is considered to be generated by the PKI entity that first comes into possession of it (e.g., the Subscriber, an RA, or a CA).

Keys and random numbers for Medium Hardware key material shall be generated in [FIPS 140] Level 2 validated hardware cryptographic module.

A private key shall not appear outside of the module in which it was generated unless it is encrypted and access control in accordance with Section 6.2.6.

CA cryptographic keying material shall be generated in [FIPS 140] Level 2 validated hardware cryptographic modules.

For CAs other than Internal NPE CAs, the CA key generation shall be under two-person control. The procedures used to generate the CA keys shall be documented and signed by two or more individuals to provide auditable evidence that the documented procedures were followed. The documentation of the procedure shall be detailed enough to show that appropriate role separation was used. Independent third party (e.g., Compliance Auditor) shall validate the key generation procedures either by witnessing or by examining the signed and documented procedures.

OCSP Responder cryptographic keying material shall be generated in [FIPS 140] Level 2 validated cryptographic modules.

Medium Assurance key pairs shall be generated in [FIPS 140] Level 1 validated cryptographic modules.

Medium Hardware signature key pairs shall be generated on the Subscriber token which shall be a [FIPS 140] Level 2 validated hardware cryptographic module.

Medium Hardware encryption key pairs shall be generated on a [FIPS 140] Level 2 validated hardware cryptographic module. The hardware module need not be the Subscriber token as long as there are assurances that no copies other than the authorized key escrow copy of the private encryption key continue to exist after the generation and transfer processes have completed. See Section 6.2.6 for transfer of private keys.

6.1.2 Private Key Delivery to Subscriber

If the Subscriber is not in possession of the Subscriber's hardware cryptographic module when keys are generated on the token, the cryptographic module shall be delivered to the Subscriber using secure and accountable means.

The cryptographic module shall be kept inactive while in transit and shall only be activated upon receipt of acknowledgement from the Subscriber. The CMA shall maintain a record of acknowledgement of receipt by the Subscriber.

If the Subscriber is not in possession of private keys when the keys are generated, the keys shall be transmitted or delivered to the Subscriber in encrypted form in compliance with the requirements of Section 6.2.8. The Subscriber shall acknowledge receipt of the private key. The originally generated private signature and/or authentication key shall be destroyed. Mechanisms shall ensure that additional copies of keys are not maintained except as allowed in this CP.

Keys associated with Medium Hardware shall be transmitted and delivered such that they can only be used and/or appear in plaintext in the target hardware cryptographic module.

6.1.3 Public Key Delivery to Certificate Issuer

Public keys shall be delivered to the certificate issuer in a way that binds the applicant's verified identification to the public key being certified. This binding shall be accomplished using means that are as secure as the security offered by the keys being certified. The binding shall be accomplished using cryptographic, physical, procedural, and other appropriate methods. The methods used for public key delivery shall be described in the CPS.

6.1.4 CA Public Key Delivery to Relying Parties

The PKI and the relying parties must work together to ensure the authenticated and integral delivery of Trusted Certificates (e.g., Self-Signed Root CA certificates). Acceptable methods for Trusted Certificate delivery include, but are not limited to:

- CAs or RAs loading Trusted Certificates onto tokens delivered to relying parties via secure mechanisms;
- secure distribution of Trusted Certificates through secure out-of-band mechanisms;
- comparison of trusted certificate hashes or fingerprints against Trusted Certificate hashes or fingerprints made available via authenticated out-of-band means (note that fingerprints or hashes posted in-band along with the certificate are not acceptable as an authentication mechanism); and/or,
- downloading trusted certificates from secure/trusted web sites secured with a currently valid DoD certificate of equal or greater assurance level than the certificate being downloaded.

6.1.5 Key Sizes

With the exception of OCSP Responder Certificates, all certificates shall contain a public key and be signed using a key size and hash algorithm that is at least as strong as that required for the highest assurance policy OID asserted in the certificate. RSA 2048 bit certificates and CRLs shall not be valid beyond 31 December 2030.

Highest Policy	Minimum RSA Key	Minimum ECC Key*	Minimum Hash
Medium-112	2048	256	SHA-256
Medium-128	3072	256	SHA-256
Medium-192	7680	384	SHA-384
Internal NPE	2048	256	SHA-256

Table 6-1

*For additional minimum ECC Key information, see Section 7.

All CRLs and OCSP Responder certificates shall be signed with the same signature algorithm, key size, and hash algorithm used by the CA to sign other certificates.

CAs may issue OCSP Responder certificates with a public key that is acceptable as specified in Table 4 of [SP 800-57] for the anticipated key life.

OCSP Responders shall sign responses using a signature algorithm, key size, and hash algorithm of equal or greater cryptographic strength than are acceptable as specified in Table 4 of [SP 800-57] for the anticipated key life.

6.1.6 Public Key Parameters Generation and Quality Checking

Public key parameters shall always be generated and checked in accordance with the standard that defines the cryptographic algorithm in which the parameters are to be used.

6.1.7 Key Usage Purposes (as per X.509 V3 Key Usage Field)

Certificates issued, including the key usage extension in the certificates, shall comply with Section 7.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

Cryptographic modules shall be validated to the [FIPS 140] levels listed in Table 6-2 below.

Assurance Levels	CA	OCSP	CMS	RA (or TA)	Subscriber
Medium Software	Level 2*(Hardware)	Level 2 (Hardware)	N/A	Level 2 (Hardware)	Level 1
Medium Hardware	Level 2*(Hardware)	Level 2 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)
Medium NPE	Level 2*(Hardware)	Level 2 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)	Level 1
Internal NPE	Level 2 (Hardware)	Level 1	N/A	Level 2 (Hardware)	Level 1

Table 6-2

* Level 3 Physical Security

Code signing keys shall be in Level 2 (Hardware).

Content signing keys shall be in Level 2 (Hardware).

All cryptographic modules shall be operated such that the private keys are never output in plaintext.

When a single cryptographic module has the private keys of more than one entity, the private keys shall be protected in a cryptographic module validated at [FIPS 140] Level 2 hardware or higher. Where an entity controls a cryptographic module that has multiple private keys for certificates of different types or with different DNs that have been issued to or provided to that entity by the PKI, this requirement shall not apply.

No one shall have access to a private signing key but the Subscriber.

Cryptographic modules, shall be protected from unauthorized access at all times, including when activated. Hardware cryptographic modules shall be removed and stored when not in use.

The Card Management Master Key shall also conform to [SP 800-78] requirements. Diversification operations shall also occur on the Hardware Security Module (HSM). Activation of the Card Management Master Key shall require strong authentication of Trusted Roles. Card management shall be configured such that only the authorized CMS can manage issued cards.

All cryptographic module shall be deactivated or destroyed when no longer valid; deactivation of the cryptographic module may be conducted manually or automatically (e.g., after a period of in activity or based on revocation).

For hardware cryptographic modules issued to Trusted Roles, all cryptographic hardware tokens shall be surrendered to their CMA prior to leaving the organization. The token shall be zeroized or destroyed promptly upon surrender and shall be protected from malicious use between surrender and zeroization or destruction.

For hardware cryptographic modules issued to other Subscribers, the cryptograpic hardware token shall either be surrendered or Subscribers will destroy private signature keys when no longer needed/when expired/when revoked.

Private keys (including Backup copies) shall be destroyed when they are no longer needed.

The encrypted form of the private key shall be protected from unauthorized access or copying.

Subscribers shall be responsible for the protection of their own private keys and associated cryptographic module.

NPE PKI Sponsors shall be responsible for all copies of the NPE private keys and associated cryptographic modules.

For Group or Role certificates, Subscribers (members of the Group or Role) shall be responsible for the private keys and associated cryptographic modules that they are assigned. PKI Sponsors for Group/Role shall be responsible for ensuring control of the private key(s) and associated cryptographic module(s).

6.2.2 Private Key (n out of m) Multi-Person Control

Internal NPE CAs have no multi-person control requirements.

For all other policies, the following multi-person controls shall apply:

- CA and OCSP Responder key generation, key activation and key backup shall require the presence of two Trusted Roles as defined in Section 5.2.1. For these activities, one of the Trusted Roles shall be a system administrator. The other party shall not hold the ISSO or Compliance Auditor role.
- access to CA and OCSP Responder signing keys backed up for disaster recovery shall be under at least two-person control.
- the CA and OCSP Responder certificate request (including the public key generation and delivery) for the purpose of generating a CA or OCSP certificate shall be carried out under two-person control. The names of the parties used for two-person control shall be maintained on a list that shall be made available for inspection during compliance audits.
- Third party key recovery of escrowed private key shall be performed and kept under two-person control until the key is delivered to the third party.

6.2.3 Private Key Escrow

Private keys, except for decryption private keys, shall not be escrowed. All human Subscriber, group, and role decryption private keys shall be escrowed. NPE decryption private keys may be escrowed. Key escrow shall be carried out in accordance with the requirements specified in Section 4.12.1.

Only decryption private keys may be escrowed in accordance with the requirements specified in Section 4.12.1.

6.2.4 Private Key Backup

Subscribers are permitted to backup their own encryption (but not signature) private keys. Backup of a Subscriber's private signature keys for the sole purpose of key recovery shall not be made. Subscribers are permitted to make operational copies of private keys residing in software cryptographic modules for each of the Subscriber's applications or locations that require the key in a different location or format.

NPE PKI Sponsors (see Sections 3.2.3 and **Error! Reference source not found.**) are authorized to make a s ingle backup copy of the NPE private keys residing in software to support backup in cases where the NPE malfunction results in key corruption.

All key transfers shall comply with the requirements of Section 6.2.6. The Subscriber (PKI Sponsor for NPE) shall be responsible for ensuring that all copies of private keys (including those that might be embedded in NPE backups) are protected commensurate with the same protections as the online private keys (including protecting any workstation on which any of its private keys reside).

CA private signature keys shall be backed up. Backup copies shall be handled under the same multi-person control as the original signature key. No more than two backup copies of the CA private signature keys shall be made. One copy of the backup shall be kept at a backup location.

OCSP Responder's private signature keys may be backed up. Backup copies shall be handled under the same multi-person control as the originail signature key. No more than two backup copies of the OCSP Responder's private signature keys shall be made.

6.2.5 Private Key Archival

Private keys shall not be copied beyond the requirements stipulated in Sections 5.5,1, 6.2.3, and 6.2.4.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

In the event that a private key is to be transported from one cryptographic module to another, the private key shall be encrypted during transport. Cryptographic strength of the encryption shall be commensurate with the cryptographic strength of the key being transported.

The encrypted form of the private key being transported shall be protected from unauthorized access or copying. Encrypted copies shall be removed from storage or destroyed once transferred to the destination cryptographic module.

Private or symmetric keys used to encrypt the private keys for transport shall be protected from disclosure. The protection of these keys shall be commensurate with that provided the data protected by the certificate associated with the private key being transported.

6.2.7 Private Key Storage on Cryptographic Module

Private keys stored in a cryptographic module shall be protected from unauthorized access and use in accordance with [FIPS 140] requirements applicable for the module.

6.2.8 Method of Activating Private Key

For Medium NPE and Internal NPE assurance levels, NPE private keys may be activated without entry of activation data.

For all other assurance levels and entities, passwords, PINs, biometric data, or other mechanisms of equivalent authentication robustness shall be used to activate the private key in a cryptographic module.

6.2.9 Method of Deactivating Private Key

After use, cryptographic modules shall be deactivated via a manual logout procedure or automatically after a period of inactivity.

6.2.10 Method of Destroying Private Key

Private keys associated with identity, signature, code signing, content signing, or system or device certificates that do not assert keyEncipherment or keyAgreement shall be destroyed and any keys used to transport them, where possible, when the certificates to which they correspond expire or are revoked.

For software cryptographic modules, this may be accomplished by overwriting the data with an NSA approved wiping utility.

For hardware cryptographic modules, this may be through executing a zeroizing command. NSA approved means of destruction include but are not limited to; physical destruction, zeroizing, or other means to erase the private keys. Physical destruction of hardware cryptographic modules and hardware tokens is not a requirement, though it may be necessary to render private keys unusable.

6.2.11 Cryptographic Module Rating

Requirements for cryptographic modules are as stated in Section 6.2.1.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

The public key is archived as part of the certificate archival (see Section 5.5.1).

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Table 6-3 provides the maximum validity periods and private key lifetimes for the various type of entities.

Certificate Type	Private Key Validity	Certificate Validity
Root CA	30 years	30 years
Intermediate CA	10 years	10 years
Subordinate CA	6 years	6 years
OCSP Responder (delegated model)	3 years	45 days
OCSP Responder (explicit trust model)	3 years	3 years
OCSP Responder (CA Hosted)	Up to life of issuing CA	Up to life of issuing CA
Identity/Authentication	3 years	3 years
Signature	3 years	3 years
Encryption	No limit for decryption usage	3 years
Code Signing	13 months for signing	6 years
PIV Content Signing	13 months for signing	6 years
System or Device	3 years	3 years
Internal NPE Root CA	30 years	30 years
Internal NPE Intermediate CA	20 years	10 years
Internal NPE Signing CA	10 years	10 years
Internal NPE Device	3 years	3 years

Table 6-3

The Content Signing certificate associated with the private key used to sign security objects on a CAC shall not expire before the expiration date of the certificates on the CAC.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

Activation data shall meet the “strength of authentication mechanism” requirements in [FIPS 140].

PINs, when used, shall be 6 digits at a minimum. Randomly generated PINs shall be used when possible. If this is not possible, Subscribers who create their own PINs shall be instructed to select PINs that are not related to their personal identity, history, or environment. Sequences, repeated numbers, social security numbers, and date formats, or other easily guessed numbers shall not be used.

When alphanumeric passwords are used, an interspersed mix of 8 characters, including at least two interspersed digits, shall be used. The passwords shall not resemble dictionary words; they shall differ from words or names by at least two characters that are not simple number-for-letter substitutions and shall not consist of words or names followed by 1-4 digits. The passwords shall not contain sequences, repeated characters, date formats, or license plate formats. To the extent practicable, technical means shall be used to verify that passwords meet all of the requirements in this section.

If random numbers are used to generate PINs or passwords, the random numbers shall meet all the applicable [FIPS 140] requirements. The method used to derive PIN or password characters from the random numbers shall ensure that all valid characters for the PIN or password are selected with equal probability.

6.4.2 Activation Data Protection

Activation data for cryptographic modules should be memorized, not written down. If written down, it shall be secured at the level of the data that the associated cryptographic module is used to protect and shall not be stored with the cryptographic module.

Entry of activation data shall be protected from disclosure (e.g., the data should not be displayed while it is entered).

Activation data shall not be shared with the individuals who are not authorized to activate or use the associated cryptographic module. Subscribers shall be advised to protect the activation data and not share the activation data with those who do not have a need to use it. For an individual Subscriber, they shall be instructed to not share the activation data with anyone.

If the activation data must be transmitted, it shall be transmitted via a protected channel, and distinct in time and place from the associated cryptographic module. The Subscriber shall be advised of the shipping date, method of shipping, and expected delivery date of the activation data. As part of the delivery method, Subscribers shall sign and return a delivery receipt.

6.4.3 Other Aspects of Activation Data

CMAs shall change their CMA cryptographic module activation data whenever the CMA token is returned for maintenance or re-key.

Where a single cryptographic module has the private keys of more than one entity, remote activation shall require authentication commensurate with the assurance level of the certificate of the key being activated.

When activation data (e.g., a password or Personal Identification Number (PIN)) is provided to the Subscriber, the CMA in possession of the activation data shall ensure that only the Subscriber knows the activation data. Furthermore, the CMA shall ask the Subscriber to change the activation data once the Subscriber is in control of the cryptographic module and the activation data.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

CMA equipment shall use operating systems that:

- Require authenticated logins;
- Provide discretionary access control;
- Provide a security audit capability;
- Provide process isolation; and,
- Support recovery from key or system failure.

CMA equipment shall be configured in accordance with all relevant NSA Configuration Guides and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG) or local agency equivalent.

For CAs, other than Internal NPE CAs, two-person control shall be enforced (using physical and/or technical means) on functions performed to administer the hardware, operating system, and applications.

The number of accounts and personnel assigned for CMA equipment and the administration thereof shall be the minimum number necessary to accomplish the required functions. Any management of the PKI equipment shall be performed from a single administrative domain.

For CMA equipment operated in a VME, the requirements above shall be applied to the hypervisor where applicable.

6.5.2 Computer Security Rating

No Stipulation.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

PKI hardware and software shall be developed using best commercial practices.

6.6.2 Security Management Controls

The CA CMS, and OCSP Responder equipment, including the hypervisor and the underlying hardware in a VME, shall be dedicated to administering a key management infrastructure. The configuration of the CA, CMS and OCSP Responder systems, as well as any modifications and upgrades, shall be documented. The CA, CMS and OCSP Responder systems shall not have installed applications or component software, which are not part of the CA, CMS and OCSP Responder configuration. A formal configuration management methodology shall be used for installation and ongoing maintenance of CA, CMS and OCSP Responder systems. There shall be a mechanism for detecting unauthorized modifications to the CA, CMS and OCSP Responder system software or configuration.

The CA, CMS, and OCSP Responder software shall be verified periodically to ensure the integrity of the software.

Reasonable care shall be taken to prevent malicious software from being loaded on RA equipment. Only applications required to perform the organization's mission shall be loaded on the RA computer, and all such software shall be obtained from sources authorized by local policy.

CMA equipment shall be scanned for malicious code on first use and periodically afterward.

6.6.3 Life Cycle Security Controls

Equipment (hardware and software) procured to operate PKI shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with. Equipment developed for a PKI shall be developed in a controlled environment.

All hardware and software that has been identified as supporting a CA, CMS, or OCSP Responder shall be shipped in protective packaging and delivered via controlled methods that provide a continuous chain of accountability from the location where it has been identified as supporting a CMA function to the using facility. CA, CMS, and OCSP Responder software, when first loaded, shall be verified as being that supplied by the authorized source, with no unauthorized modifications, and be the version intended for use.

If any classified application software has been loaded, or if any classified information has ever been loaded on PKI equipment or cards, the PKI equipment shall be shipped via a method providing security equivalent to the COMSEC Material Control System (CMCS).

Practice Notes:

PKI equipment (hardware and software) is not considered or labeled COMSEC or CRYPTO material PKI equipment, even after being loaded with classified information or connected to a classified environment.

PKI equipment, while not COMSEC material, should be protected to comparable standards (see [CNSSI 4005].)

6.7 NETWORK SECURITY CONTROLS

Internal NPE CAs shall be provided with network security controls equivalent to those provided to other high value assets (e.g., domain controllers) on the network.

Other CMA equipment shall be located on internal networks behind boundary/perimeter network defenses and afforded protections consistent with the *Risk Management Framework (RMF) for DoD Information Technology* [DoDI 8510.01] specified controls for network security for systems categorized in accordance with *Security Categorization and Control Selection for National Security Systems* [CNSSI 1253] having an impact of High for integrity and availability. Services allowed to and from CA, CMS, and OCSP Responder equipment shall be limited to those required to perform CMA functions. Other CMA equipment may enable additional services consistent with local policy.

Protection of CMA equipment shall be provided against known network attacks. All unused network ports and services shall be turned off. Any network software present on the CMA equipment shall be necessary to the functioning of the CMA application.

Root CA equipment shall not be connected to any other equipment using wired, wireless, or any other communications mechanism.

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

6.8 TIME STAMPING

Asserted times shall be accurate to within three minutes of an authoritative time source (as stipulated in applicable CMA CPS).

Electronic or manual procedures may be used to maintain system time.

Changes to time source and adjustments (i.e., system clock adjustments) are an auditable event (see Section 5.4.1).

7 CERTIFICATE, CRL, AND OCSP PROFILE

7.1 CERTIFICATE PROFILE

Certificate profiles are described in [DoD PROF].

For Internal NPE, certificate profiles are described in [Internal NPE CPS].

7.2 CRL PROFILE

CRL profiles are described in [DoD PROF].

For Internal NPE, CRL profiles are described in [Internal NPE CPS].

7.3 OCSP PROFILE

7.3.1 Version Number(s)

The DoD PKI shall use OCSP Version 1.

7.3.2 OCSP Extensions

Appropriate extensions from [RFC 6960] may be used in OCSP requests and responses. If a request contains a nonce and the response does not contain the nonce, the Relying Party may process the response if the information is deemed reasonably current.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

In accordance with [DoDI 8520.02], multiple DoD organizations have compliance audit responsibilities. Management of compliance audits including the following:

- DoW CIO evaluates and approves release of compliance audit letters to the FPKI or other PKI entities with which the DoD has a relationship. DoW CIO coordinates all FPKI memorandum of agreement evaluation and coordinates alignment with FPKI PA.
- DoD PKI PMO compiles all compliance audit or other assessment data for submission to the FPKI PA and NSS PKI MGB. DoD PKI PMO requests release approval via DoW CIO. DoD PKI PMO conducts all CPS compliance analysis.

In accordance with [DoDI 8520.02], facilitation of compliance audits includes participation from multiple DoD organizations. The following DoD organizations facilitate compliance audits and ensure that audit results are provided to DoD PKI PMA via the DoD PKI PMO:

- Root CA: DoD PKI PMO (on behalf of the NSA)
- Subordinate CAs: DISA
- OCSP Responders: DISA
- Internal NPE CAs: CC/S/As operating on Secret networks
- RAs: CC/S/As
- RAPIDS: DMDC
- ATIMS: DMDC
- CMS: DMDC

Compliance analysis of practice statements conducted during compliance auditing may be recorded by a Compliance Auditor; compliance analysis of DoD PKI certification practice statements is the responsibility of the DoD PKI PMA (see Section 1.5.3).

In addition to PKI requirements outlined below, DoD conducts other inspections and evaluations to support cybersecurity, accountability, and integrity of all DoD Information Networks (DODIN) entities.

Auditing responsibilities by the Security Auditor are outlined elsewhere throughout the rest of this CP. The Security Auditor role is also identified as ISSO within this CP.

8.1 FREQUENCY AND CIRCUMSTANCES OF COMPLIANCE AUDITS AND OTHER ASSESSMENT

8.1.1 Frequency and Circumstances of Compliance Audits

All CAs, OCSP Responders, and CMSs shall be subject to an initial compliance audit prior to commencing operations at a new location to confirm that they are prepared to operate in compliance with all CP and CPS requirements. CAs and OCSP Responders, and CMSs shall be audited on an annual basis thereafter.

RAs shall be audited aperiodically. The periodicity and circumstances of these audits or assessments shall be described in the applicable CPS.

The DoD PKI PMA may require aperiodic compliance audits more frequently than annually of CMAs claiming compliance with this CP. CMAs may require aperiodic compliance audits more frequently than annually in order to validate operations of the CMA or to confirm the implementation and effectiveness of a corrective action implemented as a result of a previous compliance audit.

Internal NPE CAs shall be audited on a triennial basis if no non-compliant findings were made on the prior compliance audit and no significant changes to policies, procedures, or operations occur during the three-year audit period.

8.1.2 Frequency and Circumstances of Other Assessments

CC/S/As and CMAs may perform other assessments and inspections as necessary to determine compliance with applicable practice statements, operating procedures, or other DODIN configuration requirements.

CMAs may require periodic and aperiodic inspections of CMA operations to validate that the CMA is operating in accordance with the security practices and procedures described in DoD policy and directives, including practices set forth in an associated CPS. A subordinate CMA shall facilitate any required inspection that is directed by a superior CMA.

Evaluations of PIV Card Issuer (PCI) configurations shall be conducted annually (see [FBCA CP] and [FIPS 201]).

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

A Compliance Auditor shall demonstrate competence in the field of compliance audits and shall be thoroughly familiar with the requirements of this CP and with the CMA's CPS. The Compliance Auditor shall perform compliance audits as a regular ongoing business activity. Additionally, the Compliance Auditor shall have the sufficient expertise in information security, cryptography, and DoD PKI in order to make recommendations regarding acceptable risks, mitigation strategies, and PKI best practices.

The Compliance Auditor shall provide a statement to the DoD PKI PMA to verify that they meet the specified qualifications and requirements of this role. The DoD PKI PMA may review and verify these qualifications of any Compliance Auditor.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The Compliance Auditor shall be sufficiently organizationally separated from the audited party to provide an unbiased, independent evaluation. To ensure independence and objectivity, the CA Compliance Auditor shall not have served the entity in developing or maintaining the audited entity's facility or authorship of its CPS.

The Compliance Auditor shall provide a statement to the DoD PKI PMA to verify that they meet the specified independence of this role. The DoD PKI PMA may determine if a Compliance Auditor meets this requirement.

8.4 TOPICS COVERED BY ASSESSMENT

The purpose of a compliance audit shall be to verify that the audited party is operating in accordance with all of the requirements of this CP and applicable CPS(s).

All aspects of the CMA's operation shall be subject to compliance audits.

An initial compliance audit shall verify that the CMA is prepared to commence operations in accordance with this CP and applicable CPS(s).

For subsequent annual compliance audits, all CAs and all CMSs are subject to a full compliance audit.

CMAs (other than the CAs) may be subject to a full compliance audit or undergo compliance audit using a representative sample. If a Compliance Auditor uses statistical sampling, samples must vary for subsequent compliance audits. The Compliance Auditor shall provide a statement to verify if and what type of sampling was conducted.

A Compliance Auditor of an Internal NPE CA may be conducted using sampling if compliance audits are conducted annually.

The Compliance Auditor shall review CMA records covering the entire period from the last full compliance audit.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If a Compliance Auditor finds a discrepancy between a CMA's operation and the stipulations of its CPS, the following actions shall occur:

- the Compliance Auditor shall document the discrepancy;
- the Compliance Auditor shall notify the parties identified in Section 8.6 of the discrepancy;
- the Compliance Auditor may propose a remedy, including expected time for completion
- the audited CMA shall select appropriate remedy and reports proposed corrective action plan and timeline to its CC/S/A (see Section 8.6).
- CC/S/A shall coordinate corrective action(s) with the CMA and shall provide status reporting to DoD PKI PMO (until all corrective actions have been completed; and,
- the DoD PKI PMA, in consultation with the associated CC/S/A, shall determines when all corrective actions have been completed sufficiently.

The DoD PKI PMA may require an additional compliance audit to confirm the implementation and effectiveness of the remedy to a finding.

In any instance where a discrepancy that contributes to the ongoing compromise of sensitive information is discovered, these critical findings shall be immediately reported to the DoD PKI PMA, the DoD PKI PMO, the associated CC/S/A, and to the local authority (local base commander or ISSO). The DoD PKI PMA determines if the circumstances warrant the immediate shut down of operations, and/or the revocation of associated certificates. Discrepancies that shall be reported include (but are not limited to) the following:

- detection of a successful attempt to compromise sensitive information (including classified information for Internal NPE PKI);
- detection of an overt and intentional disregard for secure operations of the system;
- detection of systematic or widespread negligence in meeting the requirements of this CP or applicable CPS(s);
- detection of any instance of negligence or error that could have led to a serious compromise or security breach;
- detection of a system configuration that causes the wide-spread public dissemination of sensitive information; and/or,
- detection of any critical discrepancies that lead to critical findings.

For additional circumstances or actions to be taken, see Section 5.7.1.

The DoD PKI PMA determines the appropriate remedy to address critical discrepancies, up to and including revocation or non-recognition of the audited party’s certificate. Upon correction of any deficiency, the DoD PKI PMA may reinstate the CMA.

8.6 COMMUNICATIONS OF RESULTS

8.6.1 Compliance Audit Report Content

The Compliance Auditor shall report the results of a CMA compliance audit to the DoD PKI PMA. This reporting shall be signed and dated by the Compliance Auditor upon submission to the DoD PKI PMA. This reporting (compliance audit letter) shall containe the following information:

- identity of the Compliance Auditor(s) performing the audit;
- competency of the Compliance Auditor(s) to perform audits;
- experience of the Compliance Auditor(s) to perform audits;
- relationship of the Compliance Auditor(s) to the audited CMA (statement of independence);
- date(s) that the audit was performed;
- period covered by the audit (period of performance);
- methodology used to conduct the compliance audit;
- documents reviewed as a part of the compliance audit (including document dates and version numbers);

- scope of the compliance audit (including identification of CMA component and specific organization that was the subject of the audit);
- statement that the operations of the CMA were evaluated for conformity to the requirements of this CP and the applicable CPS(s); and,
- summary of any findings of the compliance audit and evaluation of operational conformance to the CP, CPS or as they relate to the security and integrity of DoD PKI.

8.6.2 Compliance Audit Results Reporting

For all compliance audits, the Compliance Auditor shall provide the DoD PKI PMA and CC/S/A with the official report of the compliance audit results (including all elements outlined in Section 8.6.2).

The results of compliance audits shall be reported to the audited CMA.

Implementation of remedies shall be communicated to the DoD PKI PMA as outlined in Section 8.5.

DoD PKI PMO determines what (if any) further notifications or actions are necessary to meet the requirements of this CP or the CPS.

DoD PKI PMO coordinates via DoW CIO for reporting of compliance audit results to FPKI PA.

Results of compliance audits conducted on Internal NPE CAs operating on Secret networks shall be provided by the CC/S/As to the DoD PKI PMO as a part of DoD's Annual Summary submission to the NSS PKI MGB.

8.6.3 Assessment Reporting

For assessments or inspections with findings that might impact PKI operations, CMAs and CC/S/As shall report these results to the DoD PKI PMA.

CMAs (or associated CC/S/As) shall provide results of other assessments to Compliance Auditors upon request.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 Certificate Issuance or Renewal Fees

No stipulation.

9.1.2 Certificate Access Fees

No stipulation.

9.1.3 Revocation or Status Information Access Fees

CAs shall make current revocation information, including CRLs, available to Relying Parties at no charge.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

No stipulation.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of Business Confidential Information

Not applicable.

9.3.2 Information Not Within the Scope of Business Confidential Information

Not applicable.

9.3.3 Responsibility to Protect Business Confidential Information

Not applicable.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

All Subscriber identifying information is protected by, and shall be maintained in accordance with, the Privacy Act of 1974, as implemented by DoD Directive 5400.11, *DoD Privacy Program* [DoDD 5400.11] and DoD Regulation 5400.11-R, *DoD Privacy Program* [DoD 5400.11-R].

9.4.2 Information Treated as Private

When a CMA requests non-certificate information (e.g., identifying numbers, business or home addresses and telephone numbers) from the Subscriber, the CMA shall ensure that a Privacy Act Statement is furnished to the Subscriber as provided for in [DoD 5400.11-R].

9.4.3 Information Not Deemed Private

A certificate may contain information that is relevant and to effect secure transactions with the certificate. Such information may include, but is not limited to, Subscriber's Name, Subscriber Organization, Subscriber e-mail address, Subscriber EDI PI, etc.

9.4.4 Responsibility to Protect Private Information

Private information gathered for PKI purposes shall only be used to manage Subscriber certificates. Private information shall be protected in accordance with requirements set forth in [DoD 5400.11-R].

All private information collected as part of the identity proofing process shall be protected to ensure confidentiality and integrity. CMAs are 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

DoD is not required to provide any notice or obtain the consent of the Subscriber in order to release the Subscriber information provided release, either within or without the Department, as authorized by [DoD 5400.11-R].

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

A CMA shall not disclose Subscriber sensitive information to any third party except as authorized by [DoD 5400.11-R].

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 INTELLECTUAL PROPERTY RIGHTS

The US DoD shall retain ownership and all intellectual property rights for any public key certificates and private keys that it issues. CAs shall not knowingly violate intellectual property rights held by others.

9.6 REPRESENTATIONS AND WARRANTIES

CMAs may not disclaim any responsibilities described in this CP.

9.6.1 CA Representations and Warranties

A CA shall conform to the stipulations of this CP, including:

- providing to the DoD PKI PMA a CPS, as well as any subsequent changes, for conformance assessment;
- conforming to the stipulations of the approved CPS;
- ensuring that registration information is accepted only from RAs who understand and are obligated to comply with this policy;
- including only valid and appropriate information in the certificate, and maintaining evidence that due diligence was exercised in validating the information contained in the certificate;
- ensuring that obligations are imposed on Subscribers in accordance with Section 9.6.3, and informing Subscribers of the consequences of not complying with those obligations;
- revoking the certificates of Subscribers found to have acted in a manner counter to those obligations;
- ensuring that obligations are imposed on non-US Government Subscribers in accordance with the provisions of Section 9.8;
- operating or providing for the services of an on-line repository that satisfies the obligations under Section 2, and informing the repository service provider of those obligations if applicable;
- posting certificates and CRLs to the repository; and,
- protecting escrowed copies of private keys from unauthorized disclosure.

A CA who is found to have acted in a manner inconsistent with these obligations is subject to action as described in Section 8.5.

OCSP Responders shall ensure the following:

- certificate and revocation information is accepted only from valid CAs; and,
- include only valid and appropriate responses, and maintain evidence that due diligence was exercised in validating the certificate status.

An OCPS Responder what that is found to have acted in a manner inconsistent with these obligations is subject to action as described in Section 8.5.

A CMS shall conform to the stipulations of this CP, including:

- providing a CPS to the DoD PKI PMA, as well as any subsequent changes, for conformance assessment;
- conforming to the stipulations of the approved CPS;
- ensuring that registration information is accepted only from RAs who understand and are obligated to comply with this policy;
- including only valid and appropriate information in certificate requests, and maintaining evidence that due diligence was exercised in validating the information contained in the certificate;
- ensuring that obligations are imposed on Subscribers in accordance with Section 9.6.3, and informing Subscribers of the consequences of not complying with those obligations;
- revoking the certificates of Subscribers found to have acted in a manner counter to those obligations;
- ensuring that obligations are imposed on non-US Government Subscribers in accordance with the provisions of Section 9.8; and,
- protecting escrowed copies of private keys from unauthorized disclosure.

A CMS who is found to have acted in a manner inconsistent with these obligations is subject to action as described in Section 8.5.

9.6.2 RA Representations and Warranties

An RA who performs registration functions as described in this policy shall comply with the stipulations of this policy and comply with a CPS approved by the DoD PKI PMA for use with this policy. An RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities.

The division of PKI duties between the CA and RA may vary among implementations of this certificate policy as provided in the CA's CPS. Any RA shall conform to the stipulations on this CP, including the following:

- maintaining its operations in conformance to the stipulations of the approved CPS;
- including only valid and appropriate information in certificate requests, and maintaining evidence that due diligence was exercised in validating the information contained in the certificate; and,
- ensuring that obligations are imposed on PKI Sponsors in accordance with Section 9.6.3, and that PKI Sponsors are informed of the consequences of not complying with those obligations.

9.6.3 Subscriber Representations and Warranties

Subscribers shall:

- accurately represent themselves in all communications with the PKI;
- protect their private keys at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements, and local procedures;
- notify, in a timely manner, the CMA that issued their certificates of suspicion that their private keys are compromised or lost. Such notification shall be made directly, or indirectly through mechanisms consistent with the CA's CPS;
- abide by all the terms, conditions, and restrictions levied upon the use of their private keys and certificates;
- upon notification of the recovery of an escrowed private key, determine if revocation of the associated certificate is necessary, and request the revocation if needed; and,

- use certificates provided by the DoD PKI only for transactions related to DoD business.

PKI Sponsors (as described in Section **Error! Reference source not found.**) assume the obligations of S ubscribers for the certificates associated with their components. A PKI Sponsor shall be required to confirm that they will meet respecting protection of the private key and use of the certificate before being issued the certificate.

Group/Role PKI Sponsors shall maintain a current and accurate list of all persons assigned to the group/role. The Group/Role PKI Sponsors shall track physical possession of any shared token within the group/role.

9.6.4 Relying Party Representations and Warranties

See Section 4.5.2.

9.6.5 Representations and Warranties of Other Participants

Third party requestors of escrowed keys shall be bound, by legal and policy means, to the key protection and other provisions of this CP.

Repositories that support a CA in posting information as required by this policy shall:

- maintain availability of the information as required by the certificate information posting and retrieval stipulations of this policy; and,
- provide access control mechanisms sufficient to protect repository information as described in Section 2.4.

-

9.7 DISCLAIMERS OF WARRANTIES

There are no implied or express warranties associated with DoD PKI products and services.

9.8 LIMITATIONS OF LIABILITY

The U.S. Government shall not be liable to any party for the operation of DoD PKI. All parties shall hold the NSA harmless for its operation of the Root CA.

9.9 INDEMNITIES

No stipulation.

9.10 TERM AND TERMINATION

9.10.1 Term

This CP shall remain in effect until either a new DoD X.509 CP is approved by the DoD PKI PMA or the DoD PKI is terminated. This CP is reviewed annually. If there are no changes during a triennial period, the DoD PKI PMA shall document the continued use of the current version.

9.10.2 Termination

This CP shall survive any termination of the CA. The requirements of this CP remain in effect through the end of the archive period for the last certificate issued.

9.10.3 Effect of Termination and Survival

The responsibilities for protecting business confidential and personal information and DoD's intellectual property (IP) rights shall survive termination of this CP. The responsibilities for protecting business confidential and PII, and for protecting IP rights, shall survive termination of this CP.

The archive requirements of this CP remain in effect through the end of the archive period for the last certificate issued. Other requirements concerning the organization and operations of DoD PKI; certificate application, usage, and revocation; physical and technical security controls; audits; and other business and

legal matters shall remain in effect through the expiration date of the last certificate issued and/or cessation of operations and closure of the DoD PKI. See Section 5.8.1 for additional requirements.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

The DoD PKI PMA shall establish appropriate procedures for communications with cross-certified CAs.

Any CMA personnel may be removed from their duties by their supervisor. Notice is effective when given; oral notification will be confirmed in writing. For CA termination, see Section 5.8.1. For RA termination, see Section 5.8.2. For TA termination, see Section 5.8.3.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

The DoD PKI PMA shall review this policy at least once every year. Errors, updates, or suggested changes to this document shall be communicated to the contact in Section 1.5.2. Such communication must include a description of the change, a change justification, and contact information for the person requesting the change.

The DoD PKI PMA shall publish information (including this policy) on a web site, consistent with DoD policies regarding web site contents.

The DoD PKI PMA will maintain a list of CAs asserting this policy (this responsibility may be delegated to a Root- or Intermediate-CA in practice). Certificate Policy updates shall be sent to those CAs. The CMA shall notify its Subscribers of any changes to the certificate policy via a mechanism described in its CPS.

9.12.2 Notification Mechanism and Period

All policy changes under consideration by the DoD PKI PMA shall be disseminated to interested parties for a period of at least one month.

The DoD PKI PMA shall accept, accept with modifications, or reject the proposed change after completion of the review period.

9.12.3 Circumstances Under Which OID Must be Changed

The policy OID shall only change if the change in the CP results in a material change to the trust by the non-DoD relying parties.

9.13 DISPUTE RESOLUTION PROVISIONS

The DoD PKI PMA shall decide any disputes over the interpretation or applicability of the DoD PKI CP.

9.14 GOVERNING LAW

The laws of the United States of America shall govern this policy.

9.15 COMPLIANCE WITH APPLICABLE LAW

The PKI participants shall comply with applicable laws.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

Should it be determined that one section of this policy is incorrect or invalid, the other sections shall remain in effect until the policy is updated. Requirements for updating this policy are described in Section 9.12.1. Responsibilities, requirements, and privileges of this document are merged to the newer edition upon release of that newer edition.

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 OTHER PROVISIONS

No stipulation.

10 ACRONYMS AND DEFINITIONS

This policy uses the following acronyms:

AAL	Authenticator Assurance Level
ATIMS	Alternate Token Information Management System
CA	Certification Authority
CC	Common Criteria
CMA	Certificate Management Authority
CMCS	COMSEC Material Control System
CNSS	Committee on National Security Systems
COMSEC	Communications Security
CONOP	Concept of Operations (document)
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DAA	Designated Approving Authority
DISA	Defense Information Systems Agency
DMDC	Department of Defense Manpower Data Center
DN	Distinguished Name
DoD	Department of Defense
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
EAL	Evaluation Assurance Level
FBCA	Federal Bridge Certification Authority
FIPS	Federal Information Processing Standard
FPKI	Federal Public Key Infrastructure
FVEY	Five Eyes
GS	General Schedule (Federal civilian level)
HAG	High Assurance Guard
IAL	Identity Assurance Level
I&A	Identification and Authentication
ICRL	Indirect Certificate Revocation List
ID	Identity (also, a credential asserting an identity)
INE	In-Line Network Encryptor
IP	Intellectual Property
IP	Internet Protocol
ISSO	Information System Security Officer
KEA	Key Exchange Algorithm
KES	Key Escrow System
KRA	Key Recovery Agent
MD	Maryland
MGB	Member Governing Body
NEATS	NIPRNET Enterprise Alternate Token System
NIPRNET	Non-classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NPE	Non-Person Entity
NSA	National Security Agency
NSS	National Security System
NSSI	National Security System Information
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PAA	Policy Approving Authority
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PMA	Policy Management Authority

PSS	Probabilistic Signature Scheme
RA	Registration Authority
RD	Road
RSA	Rivest, Shamir, Adleman (encryption algorithm)
S/MIME	Secure Multipurpose Internet Mail Extensions
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmented Information
SIPRNET	Secret Internet Protocol Router Network
SSL	Secure Sockets Layer
STE	Suite
TA	Trusted Agent
TLS	Transport Layer Security
US	United States
VME	Virtual Machine Environment

The primary source of definitions is the *Committee on National Security Systems (CNSS) Glossary* [CNSSI 4009]; other sources are used if [CNSSI 4009] had no entry for the term, or if another source provides a definition more appropriate to PKI. If no reference is given, the definition is ad hoc.

access	Ability to make use of any information system (IS) resource. [CNSSI 4009]
access control	The process of granting or denying specific requests: (1) for obtaining and using information and related information processing services; and (2) to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances). [CNSSI 4009]
accreditation	Formal declaration by a designated accrediting authority (DAA) or principal accrediting authority (PAA) that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards. [CNSSI 4009]
activate	To make a cryptographic module operative by providing activation data to cryptographic module in order to permit an authenticated operator to perform one or more of the services allowed within an authorized role
activation data	A password, personal identification number (PIN), biometric data, or other mechanisms of equivalent authentication robustness used to protect access to any use of a private key, except for private keys associated with System or Device certificates.
applicant	The Subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG, footnote 32]
Approving Authority	Senior-level official within a U.S. Service, DoD Agency, or Civil Department/Agency who is responsible for approving the establishment of CA operations within their respective organizations.
archive	Long-term, physically separate storage.
Attribute Authority	An entity recognized by a CMA 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. [CNSSI 4009]

audit data	A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security relevant transaction from inception to final result. [CNSSI 4009, "audit trail"]
Authenticator Assurance Level	A measure of the strength of an authentication mechanism and, therefore, the confidence in it, as defined in [SP 800-63] in terms of three levels: AAL1 (Some confidence), AAL2 (High confidence), and AAL3 (Very high confidence) [FIPS 201-03]
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. [CNSSI 4009]
Authorizing Official	A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. [CNSSI 4009]
backup	Copy of files and programs made to facilitate recovery if necessary. [CNSSI 4009]
binding	Process of associating two related elements of information. [CNSSI 4009]
biometric	A physical or behavioral characteristic of a person.
CA facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
CA Hosted OCSP Responder	An OCSP Responder that is collocated with the CA and is hosted in the CA Enclave with protection equivalent to that provided to the CA signing key.
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]
Certificate Management Authority (CMA)	A Certification Authority, Registration Authority, Local Registration Authority, or OCSP Responder that has been issued a DoD PKI certificate.
certificate-related information	Information, such as a Subscriber's postal address, that is not included in a certificate, but that may be used by a CA in certificate management.
Certificate Status Authority	A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.
Certification Authority (CA)	An authority trusted by one or more users to create and assign certificates. [ISO 9594-8]
client (application)	A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.
compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or

	unintentional disclosure, modification, destruction, or loss of an object may have occurred. [CNSSI 4009]
confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [CNSSI 4009]
CRL scope	The set of certificates that could appear on a given CRL. Each CRL has a particular scope. For example, the scope could be "all certificates issued by CA X", "all CA certificates issued by CA X", "all certificates issued by CA X that have been revoked for reasons of key compromise and CA compromise", or a set of certificates based on arbitrary local information, such as "all certificates issued to the NIST employees located in Boulder". [RFC 5280]
cryptographic module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS 140]
cryptoperiod	Time span during which each key setting remains in effect. [CNSSI 4009]
dual use certificate	A certificate that is intended for use with both digital signature and data encryption services.
e-commerce	The use of network technology (especially the Internet) to buy or sell goods and services.
encrypted network	A network that is protected from outside access by NSA approved high-grade (Type I) cryptography.
encryption certificate	A certificate containing a public key that is used to encrypt or decrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes. The process of storing protecting and escrowing the private component of the key pair associated with the encryption certificate is sometimes referred to as key management. An encryption certificate asserts a key usage of key encipherment or key agreement.
firewall	Gateway that limits access between networks in accordance with local security policy. [CNSSI 4009]
High Assurance Guard (HAG)	An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.
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 Assurance Level (IAL)	A category that conveys the degree of confidence that a person’s claimed identity is their real identity, as defined in [SP 800-63] in terms of three levels: IAL1 (Some confidence), IAL2 (High confidence), and IAL3 (Very high confidence) [FIPS 201-03]

Identity Proofing	The process of providing sufficient information (e.g., identity history, credentials, documents) to establish an identity. [FIPS 201-3]
Information System Security Officer (ISSO)	Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program. [CNSSI 4009]
insider threat	An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.
integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [CNSSI 4009]
intellectual property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.
key escrow	The retention of the private component of the key pair associated with a Subscriber's encryption certificate to support key recovery.
key exchange	The process of exchanging public keys (and other information) in order to establish secure communication.
key generation material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
Local Registration Authority (LRA)	A type of Registration Authority with responsibility for a local community.
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 information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, 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). [CNSSI 4009]
NIPRNET	Non-classified Internet Protocol Router Network; part of the Defense Information Infrastructure.
nonce	A random or non-repeating value that is included in data exchanged by a protocol, usually for the purpose of guaranteeing the transmittal of live data rather than replayed data, thus detecting and protecting against replay attacks. [CNSSI 4009]
non-repudiation	Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given

	individual took a particular action such as creating information, sending a message, approving information, and receiving a message. [CNSSI 4009]
Non-Person Entity (NPE)	Workstations, guards and firewalls, routers, in-line network encryptors (INEs), services and applications (e.g., database, FTP, web service), and other infrastructure components.
OCSP Responder	A trusted entity that provides on-line revocation status of certificates to Relying Parties. The OCSP Responder is either explicitly trusted by the Relying Party, or through a CA that Relying Party trusts, or through the CA that issued the certificate whose revocation status is being sought.
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 has no electronic connection to individuals outside a physically controlled space.
PKI Sponsor	Fills the role of a Subscriber for non-human system components or organizations that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this document.
Policy Management Authority (PMA)	Body or individual established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies.
privacy	State in which data and system access is restricted to the intended user community and target recipient(s).
Public Key Infrastructure (PKI)	Framework established to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	Entity responsible for identification and authentication of certificate subjects that have automated equipment for the communication of applicant data to Certification Authorities and does not sign or directly revoke certificates.
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.
re-key (a certificate)	To create a new certificate with the same name and authorizations as the old one, but with a new key, extended validity period and new serial number.
Relying Party	An 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, or system or device; the integrity of a digitally signed message; the identity of the creator of a message; or confidential communications with the Subscriber. [CNSSI 4009]
renew (a certificate)	To create a new certificate with the same name, key and authorizations as the old one, but with an extended validity period and new serial number.
repository	A trustworthy system for storing and retrieving certificates or other information relevant to certificates. [ABADSG] A repository may be a

	single system or multiple distributed systems acting as a single logical system.
risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
risk tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
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.
SIPRNET	Secret Internet Protocol Router Network; part of the Defense Information Infrastructure.
subordinate CA	In a hierarchical PKI, a CA whose certificate signing key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA.)
Subscriber	An entity that (1) is the subject named or identified in a certificate issued to such an entity, and (2) holds a private key that corresponds to a public key listed in that certificate. [ABADSG] Current Subscribers possess valid DoD-issued certificates.
superior CA	In a hierarchical PKI, a CA who has certified the certificate signing key of another CA, and who constrains the activities of that CA. (See subordinate CA.)
system equipment configuration	A comprehensive accounting of all system hardware and software types and settings.
system high	The highest security level supported by an information system. [CNSSI 4009]
technical non-repudiation	The contribution public key mechanisms make 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. [CNSSI 4009]
trust anchor	See Trusted Certificate.
trust list	Collection of Trusted Certificates used by Relying Parties to authenticate other certificates.
Trusted Agent	Entity authorized to act as a representative of a Certificate Management Authority in performing Subscriber identity validation during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.

trusted certificate	A certificate that is trusted by the Relying Party on the basis of secure, 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.
two person control	The continuous surveillance and control of material at all times by a minimum of two authorized individuals, each capable of detecting incorrect or unauthorized procedures with respect to the task being performed and each familiar with established security requirements. [CNSSI 4009]
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	A computer system that provides the functionality of a physical machine in a platform-independent environment. It provides the functionality needed to execute an entire operating system.
zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS 140]

11 REFERENCES

This policy references the following documents:

ABADSG	American Bar Association, *Digital Signature Guidelines,* 1 August 1996.
COMMON	X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, V 2.12, August 4, 2025.
CNSSI 1253	CNSS Instruction 1253, *Security Categorization and Control Selection for National Security Systems*, 27 March 2014.
CNSSI 4005	CNSS Instruction 4005, *Safeguarding Communications Security (COMSEC) Facilities and Materials*, 22 August 2011 (with amendments).
CNSSI 4009	CNSS Instruction 4009, *Committee on National Security Systems (CNSS) Glossary*, 6 April 2015.
DoD 5400.11-R	DoD Regulation 5400.11, *DoD Privacy Program*, 14 May 2007.
DoDD 5400.11	DoD Directive 5400.11, *DoD Privacy Program*, 29 October 2014.
DoDI 5015.02	DoD Instruction 5015.02, *DoD Records Management Program*, 17 August 2017.
DoDI 8500.01	DoD Instruction 8500.01, *Cybersecurity*, 14 March 2014.
DoDI 8510.01	DoD Instruction 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*, 12 March 2014.
DoDI 8520.02	DoD Instruction 8520.02, *Public Key Infrastructure and Public Key Enabling*, 18 May 2023.
DoDI 8520.03	DoD Instruction 8520.03, *Identity Authentication for Information Systems*, 19 May 2023.
DoD PROF	*DoD PKI NIPRNet Certificate and Certificate Revocation List Profiles*, Version 7, 17 July 2025.
FBCA	X.509 Certificate Policy for the Federal Bridge Certificate Policy, V3.8, August 4, 2025.
FIPS 140	NIST FIPS PUB 140-3, *Security Requirements for Cryptographic Modules*, 22 March 2019.
FIPS 186	NIST FIPS PUB 186-4, *Digital Signature Standard*, 27 July 2013.
FIPS 201	NIST FIPS PUB 201-3, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, January 2022.
FPKI PROF	*Common Policy X.509 Certificate and Certificate Revocation List (CRL) Profiles*, Version 2.4, 04 August 2025.
ITU X.501	International Telecommunications Union (ITU) X.509: Information Technology – Open Systems Interconnection – Directory: Operational Bindings Management Protocol (DOP)
ITU X.509	International Telecommunications Union (ITU) X.509: Information Technology – Open Systems Interconnection – The Directory: Public Key and Attribute Certificate Frameworks X.509 Version 3 Public Key Certificates
ISO 9594-8	*Information Technology-Open Systems Interconnection-The Directory: Part 8: Public-key and Attribute Certificate Frameworks*, May 2017.
NARA GRS	National Archives and Records Administration, *General Records Schedule 3.2: Information Systems Security Records* (Items 060-062), January 2023.
PKCS 1	RSA Laboratories, *RSA Cryptography Standard*, Version 2.2, 27 October 2012.
RFC 3647	*X.509 Internet Public Key Infrastructure Certificate Policy and Certification Practices Framework*, November 2003.
RFC 4210	*Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)*, September 2005.
RFC 5280	*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, May 2008.

RFC 5322	Internet Message Format (IMF), October 2008
RFC 6960	*X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*, June 2013.
SP 800-57	NIST Special Publication 800-57, *Recommendation for Key Management – Part 1: General (Revision 5)*, May 2020.
SP 800-63	NIST Special Publication 800-63-3, *Digital Identity Guidelines*, June 2017 (updates as of 02 March 2020).
SP 800-78	NIST Special Publication 800-78-4, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, May 2015.
SP 800-79	NIST Special Publication 800-79-2, *Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)*, July 2015.
SP 800-157	NIST Special Publication 800-57, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*, December 2014.

12 SUMMARY OF CHANGES TO DOD X.509 CERTIFICATE POLICY, VERSION 10

Version 10.1, 19 February 2010

Change	Sections	Change Summary
2009-01	4.9.13 - 4.9.16	Added certificate suspension and restoration requirements.

Version 10.2, 4 May 2011

Change	Sections	Change Summary
2011-01	Multiple	Added a medium NPE assurance level.

Version 10.3, 16 February 2012

Change	Sections	Change Summary
2011-02	4.9.3	Allowed an automated process from an authoritative data source to request revocations without a human in the loop.
2011-03	Multiple	Added Medium Assurance OIDs at 112 and 128 bits of cryptographic strength; renamed High Assurance to FORTEZZA and realigned or removed all High Assurance requirements; added a Peer Interop OID to allow for identification of external PKIs that are not comparable with Medium Assurance but with which DoD decides to cross certify.
2011-04	1.4	Aligned the Certificate Usage section with DoD Instruction 8520.03.

Version 10.4, 21 June 2012

Change	Sections	Change Summary
2012-01	Multiple	Added DoD Key Recovery Policy requirements.

Version 10.5, 23 January 2013

Change	Sections	Change Summary
2012-02	1.5.4, 2.2, 5.3.1, 5.4.1, 5.5.5, 6.8	Clarified requirements for compliance to the Federal Bridge CP: compliance analyses performed by an independent party; publish cross certificates issued by or to the PKI; trusted roles supporting CA operations held by US Citizens; set time on the PKI and make audit entries when time is changed.
2012-03	6.2.3, 10	Clarified which private keys may be escrowed.
2012-04	3.2.3.3	Added a requirement related to a change of PKI Sponsor.
2012-05	5.6	Removed the restriction on CA signing key usage relative to the maximum life of Subscriber certificates.
2012-06	6.2.6	Added a requirement to remove PKCS #12 files from Subscriber systems.
2012-07	6.1.5, 6.1.7, 10	Clarified the requirements related to single vs. dual use certificates for applications, and clarified which certificates may have non-repudiation.

Version 10.6, 20 May 2018

Change	Sections	Change Summary
2016-01	7.2.1	Restricted CAs to only issue Version 2 Certificate Revocation Lists.
2016-02	1.2, 6.1.5, 7.1.3	Added new certificate policy OIDs and requirements for issuing certificates with 192 bits of security.
2016-03	Multiple	Deprecated the use of the FORTEZZA certificate policy OID.
2016-05	1.2, 3.2.5	Added new certificate policy OID and requirements for issuing certificates that identify system administrators.
2017-01	Multiple	Added new certificate policy OIDs and requirements for the DoD Internal NPE PKI.
2018-01	6.2.1, 6.4.3	Added requirements for protecting private keys for multiple end entities when aggregated in a single cryptographic module.
2018-02	5.4, 5.4.1, 5.5, 6.5.1, 6.6.2, 10	Added specific controls for the use of a Virtual Machine Environment to support CA or RA systems.
2018-03	4.9.3	Changed the requirement for direct CMA action to perform revocation to allow for more flexibility in how revocations are processed.
2018-04	Multiple	Editorial updates and changes required by updates to referenced documents.
2018-05	Multiple	Allowed RCVS to obtain Delegated Trust Model certificates from Elliptic Curve Cryptography CAs; accounted for Delegated Trust Model certificates automatically issued by Red Hat CAs on initially stand up; removed references to High Volume and Low Volume responders; simplifies key size and algorithm OID requirements.

Version 10.7, 3 June 2021

Change	Sections	Change Summary
2020-01	1.2, 1.4.1, 6.1.7, & 7.1.3	Add the Common Policy OIDs that are asserted in certificates issued by the DoD PKI. Deprecate the “DoD PIV” OIDs which were added, but never used.
2020-02	1.2, 4,9,3, 6.1.5, 7.1.3	Make changes to the CP to clarify that DoD is no longer issuing certificates that use SHA-1 or RSA 1024.
2021-01	1.2, 3.2.4	Add the Federal Common Policy Framework (Common CP) Derived Personal Identification Verification (PIV) Policy Object Identifiers (OID) to the DoD CP.

Version 11, 15 December 2025

Change	Sections	Change Summary
2024-2025	All CP	20240214-20250611: CPMWG review and re-write activity conducted.
	All CP	20250611: CPMWG endorses draft version 11 (substantive update) for approval by DoD PKI PMA.
	All CP	20250808: Edited version (administrative & formatting fixes) submitted to DoD PKI PMA (DoD CIO) for approval.
	All CP	20251215: DoD PKI PMA (DoW CIO) approval; title changed to DoD/DoW PKI CP based on approval memo.
	All CP	20251224: Pre-publication editing completed.