X.509 Certificate Policy
for the
United States Department of Defense

11 December 2003

Version 8.0

Prepared by:

DoD Public Key Infrastructure Program Management Office

Approved:

for **Assistant Secretary of Defense**
(Networks and Information Integration)

This Page Intentionally Left Blank

REFERENCES

The following documents contain information, which has been required by reference or which, otherwise describe or govern Department of Defense (DoD) Public Key Infrastructure (PKI) operation:

DoD5200R	*DoD 5200.2-R, Personnel Security Program.*
GIG IA Policy	DoD Chief Information Officer (CIO) Guidance and Policy Memorandum No. 6-8510 "Department of Defense Global Information Grid Information Assurance". http://www.c3i.osd.mil/org/cio/doc/gigia061600.pdf
FIPS140 (current version)	*Security Requirements for Cryptographic Modules*, 1994-01. http://csrc.nist.gov/publications/index.html
FIPS112	*Password Usage,* 1985-05-30. http://csrc.nist.gov/fips/
DITSCAP	DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process" (DITSCAP), December 30, 1997.
FIPS186-2	*Digital Signature Standard*, 2000 January 27. http://csrc.nist.gov/fips/fips186-2.pdf
FPKI-Prof	Federal PKI X.509 Certificate and CRL Extensions Profile.
KRP	*Key Recovery Policy for the United States Department of Defense,* Version 3.0, August 31, 2003.
ISO9594-8	*Information Technology-Open Systems Interconnection-The Directory: Authentication Framework,* 1997. ftp://ftp.bull.com/pub/OSIdirectory/ITU/97x509final.doc
NS4005	*NSTISSI 4005, Safeguarding COMSEC Facilities and Material*, 1997 August.
NS4009	*NSTISSI 4009, National Information Systems Security Glossary,* 1999 January.
RFC2510	Adams and Farrell. *Certificate Management Protocol,* 1999 March. http://www.ietf.org/rfc/rfc2510.txt
RFC2527	Chokhani and Ford. *Certificate Policy and Certification Practices Framework*, 1999 March. http://www.ietf.org/rfc/rfc2527.txt
RFC 2560	Myers, Ankney, Malpani, Galperin, and Adams. *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, 1999 June.*
SDN702	*SDN.702, Abstract Syntax for Utilization with Common Security Protocol (CSP), Version 3 X.509 Certificates, and Version 2 CRLs, Revision 3,* 31 July 1997. http://www.armadillo.huntsville.al.us/Fortezza_docs/sdn702rev3.pdf
SDN706	*X.509 Certificate and Certification Revocation List Profiles and Certification Path Processing Rules for MISSI Revision 3.0,* 30 May 1997. http://www.armadillo.huntsville.al.us/Fortezza_docs/sdn706r30.pdf

This Page Intentionally Left Blank

1 INTRODUCTION

The United States Department of Defense (DoD) is developing a Key Management Infrastructure (KMI) to provide engineered solutions (consisting of products and services) for security of networked computer-based systems. Part of this KMI is a Public-Key Infrastructure (PKI), consisting of products and services, which provide and manage X.509 certificates for public-key cryptography. Certificates identify the individual named in the certificate, and bind that person to a particular public/private key pair.

Programs, which carry out or support the mission of the US DoD require services such as authentication, confidentiality, technical non-repudiation, and access control. These services are met with an array of network security components such as workstations, guards, firewalls, routers, in-line network encryptors (INE), and trusted database servers. The operation of these components is supported and complemented by use of public-key cryptography. As a system solution, the components share the burden of the total system security. The use of public key certificates does not add any security services in a poorly designed or implemented system.

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 Update, Renewal, and Re-key
- Certificate token initialization/programming/management
- Privilege and Authorization Management
- System Management Functions (e.g., security audit, configuration management, archive, etc.)

The security of these services is ensured by defining requirements on PKI activities, including 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
- Definition of rules to limit liability and to provide a high degree of certainty that the stipulations of this policy are being met

The reliability of the public-key cryptography portion of the security solution is a direct result of the secure and trustworthy operation of an established PKI, including equipment, facilities, personnel, and procedures.

Electronic commerce is one important PKI application. The use of public key cryptography for electronic commerce applications should be determined on the basis of a review of the security services provided by the public key certificates, the value of the electronic commerce applications, and the risk associated with the applications. 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.

1.1 OVERVIEW

The United States Department of Defense Certificate Policy (CP) is the unified policy under which a Certificate Authority (CA) operated by a DoD component is established and operates. It does not define a particular implementation of 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. Other documents that address these issues are the DoD PKI Implementation Plan, the DoD Public Key Infrastructure Roadmap, and the DoD PKI Policy Planning Document. This document will be reviewed and updated as described in Section 8, based on operational experience, changing threats, and further analysis.

This document defines the creation and management of Version 3 X.509 public-key certificates for use in applications requiring communication between networked computer-based systems. Such applications include, but are not limited to, electronic mail; transmission of unclassified and classified information; signature of

electronic forms; contract formation signatures; and authentication of infrastructure components such as web servers, firewalls, and directories. The network backbone for these network security products may be unprotected networks such as the Internet or Nonclassified Internet Protocol Router Network (NIPRNET), or protected networks such as the Secret Internet Protocol Router Network (SIPRNET).

References are listed prior to the table of contents. A bibliography of related publications is included at the end of this document. Those publications contain information that forms the basis for public-key infrastructure. A list of acronyms follows the bibliography.

1.2 IDENTIFICATION

There are five levels of assurance in this policy, defined in subsequent sections. Each level of assurance has an object identifier (OID), to be asserted in certificates issued by CAs who comply with the policy stipulations herein. 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-class2	ID::= {id-certificate-policy 2}
id-US-dod-class3	ID::= {id-certificate-policy 5}
id-US-dod-class3hardware	ID::= {id-certificate-policy 9}
id-US-dod-class4	ID::= {id-certificate-policy 4}
id-US-dod-class5	ID::= {id-certificate-policy 6}

1.3 COMMUNITY AND APPLICABILITY

The following sections introduce the PKI and community roles involved in issuing and maintaining key management certificates. These roles are described in detail in Section 5.2.

1.3.1 PKI authorities

The **DoD Policy Management Authority** (PMA) is a body established by the Department to

- 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 Certification Practice Statements (CPS) of DoD operated CAs that offer to provide services to the DoD by analyzing the CPS documents to ensure that the practices of CAs serving the DoD comply with the DoD Certificate Policies;
- review the results of CA compliance audits to determine if the CA are adequately meeting the stipulations of approved CPS documents, and make recommendations to the CAs and to the PMA regarding corrective actions, or other measures that might be appropriate, such as revocation of CA certificates;
- 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); 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.

A **Certification Authority (CA)** is an entity authorized by the PMA to create, sign, and issue public key certificates. A CA is responsible for all aspects of the issuance and management of a certificate, including control over the registration process, the identification and authentication process, the certificate manufacturing process, publication of certificates, revocation of certificates, and re-key; and for 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. CA is an inclusive term, and includes all types of CAs. Any CA requirement expressed in this Policy applies to all CA types unless expressly stated otherwise.

In the case of a hierarchical PKI, the CAs must be subordinate to a Root-CA (and a maximum of one intermediate CA). The nature of the subordination shall be described in one or more CPSs that have been generated for that hierarchy, and implemented through procedure and certificate extensions. The CA to which a second CA is subordinate is called the second CA's "superior CA."

A **Registration Authority (RA)** is an entity that enters into an agreement with a CA to collect and verify Subscribers' identity and information, which is to be entered into public key certificates. The RA must perform its functions in accordance with a CPS approved by the CA and the PMA.

Both Certification Authorities and Registration Authorities are "Certificate Management Authorities" (CMAs). This policy will use the term CMA when a function may be assigned to either a CA or a RA, or when a requirement applies to both CAs and RAs. The term Registration Authority includes entities such as Local Registration Authorities. The division of Subscriber registration responsibilities between the CA and RA may vary among implementations of this certificate policy. This division of responsibilities shall be described in the CA's CPS.

Online Certificate Status Protocol (OCSP) Responders that comply with RFC 2560 are also CMA if issued a DoD PKI certificate.

PMA decision authority resides with Assistant Secretary of Defense, Networks and Information Integration (ASD/NII). PMA may delegate authorities in appropriate DoD policies and instructions.

1.3.2 Related authorities

CAs operating under this policy will require the services of other security, community, and application authorities, such as compliance auditors and attribute authorities. The CA shall identify, in its CPS, the parties responsible for providing such services, and the mechanisms used to support these services. More detail is given in Section 5.2.

1.3.3 End entities

1.3.3.1 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. The targeted DoD PKI Subscribers include but are not limited to the following categories of entities that may wish to communicate securely:

- DoD uniformed and civilian personnel, and eligible contractors;
- Executive department and agency personnel, and eligible contractors;
- State governments;
- Foreign government and foreign organization personnel, and eligible contractors; and
- Workstations, guards and firewalls, routers, in-line network encryptors (INE), trusted servers (e.g., database, File Transfer Protocol (FTP), and World Wide Web (WWW), and other infrastructure components. These components must be under the cognizance of humans, who accept the certificate and are responsible for the correct protection and use of the associated private key.

CAs are technically Subscribers to the PKI; however, the term Subscriber as used in this document refers only to those who request certificates for uses other than signing and issuing certificates.

1.3.3.2 Relying parties

A Relying Party is the entity who, by using another's certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate, relies on the validity of the binding the Subscriber's name to a public key. A Relying Party may use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use.

1.3.4 Applicability

Certificates asserting a Policy defined in this document 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.

Security of the Defense Information Infrastructure (DII) is of great importance to the DoD. For the DoD to effectively carry out its mission, the information must be accurate, and available when needed, only to those authorized to receive it. Furthermore, the source of information claiming to be official must be identifiable and

capable of authentication. The DoD is pursuing a layered security approach for the DII using a wide variety of security-enabled products including public key based technologies.

The DoD PKI must support the following security services: *confidentiality*, *integrity*, *authentication* and *technical non-repudiation.* The PKI supports these security services by providing Identification and Authentication (I&A), integrity, and technical non-repudiation through digital signatures, and confidentiality through key exchange. These basic security services support the long-term integrity of application data, but may not by themselves provide a sufficient integrity solution for all application circumstances. For example, when a requirement exists to verify the authenticity of a signature beyond the certificate validity period, such as contracting, other services such as trusted timestamp may be necessary. These solutions are application based, and must be addressed by Subscribers and relying parties. The PKI provides this support to a wide range of applications that protect various types of information, including:

- Administrative and Financial Information;
- National Security System Information (NSSI);
- Mission Assurance Category II (MAC II) Information;
- Mission Assurance Category I (MAC I) Information;
- Classified information up through Top Secret compartmented data.

A single solution providing support to every application would appear to be desirable but because of different legal, security and national policy requirements for protection of the different categories of information, the most cost-effective solution is one, which supports multiple assurance levels.

1.3.4.1 Level of assurance

The level of assurance associated with a public key certificate is an assertion by a CA of the degree of confidence that a Relying Party may reasonably place in the binding of a Subscriber's public key to the identity and privileges asserted in the certificate. Level of assurance depends on the proper registration of Subscribers and the proper generation and management of the certificate and associated private keys, in accordance with the stipulations of this policy. Personnel, physical, procedural, and technical security controls contribute to the assurance level of the certificates issued by a certificate management system.

1.3.4.2 Factors in determining usage

The amount of reliance a relying party chooses to place on the certificate will be determined by various risk factors. Specifically, the value of the information, the threat environment, and the existing protection of the information environment are used to determine the appropriate level of assurance of certificates required to protect and authenticate the information.

1.3.4.3 Value of the Information

The value of the information has been separated into importance of the information relative to the achievement of DoD goals and objectives, particularly the warfighter's combat mission and electronic commerce applications. This includes the sensitivity of the information (e.g., classified or sensitive), criticality (e.g., mission categories as defined by DoD 8500) or monetary value for electronic commerce applications.

Examples of data information values are:

Low Value Information:

- Mission Assurance Category III (MAC III) Data as defined in the Glossary of this CP.

Medium Value Information

- Mission Assurance Category II (MAC II) data as defined in the Glossary of this CP.
- Data protecting small and medium value financial transactions (office supplies, books, travel claims, vehicles, payroll, etc.)

High Value Information

- Mission Assurance Category I (MAC I) data as defined in the Glossary of this CP
- High value financial transactions (e.g., aircraft and building purchases)

1.3.4.4 Threat

Threat is any circumstance or event with the potential to cause harm. In terms of information systems, harm includes destruction, disclosure, or modification of data, processes, or processing components. Threats to systems include environmental disasters, physical damage, system penetration, and violation of authorization, human error, and communications monitoring or tampering. Three items to consider when assessing the threat posed by an adversary are its capability, *risk tolerance*, and access. DoD studies have concluded that a great majority of past compromises have involved *inside threats*.

1.3.4.5 Level of environmental protection

The DoD data networks on which the certificates described in this policy will be used will have various levels of protection. Examples of mechanisms that provide network protection include *network encryption*, *physical isolation*, *High Assurance Guards* (HAG), and *firewalls*. These mechanisms are used to create a collection of system high networks and enclaves. The probability of attack on protected networks is reduced because:

- access is limited to people authorized to use the network and its interconnection points with other networks (i.e., the guards or firewalls);
- even for those with access, risk tolerance must be high, due for example to the lack of anonymity on the network and its access points;
- the capabilities of an attacker inside the network are hampered by the lack of availability of "hacker tools," and the difficulty of bringing them from the outside.

The true amount of risk reduction associated with using these mitigation mechanisms can only be determined by a system security evaluation.

Examples of differing levels of environmental protection are:

Highly Protected Environment

- Networks that are protected either with encryption devices approved by the National Security Agency (NSA) for protection of classified data or via physical isolation, and that are certified for processing system-high classified data, where exposure of unencrypted data is limited to US citizens holding appropriate security clearances.

Moderately Protected Environment

- Physically isolated unclassified, unencrypted networks in which access is restricted based on legitimate need.
- Networks protected by NSA approved Type 1 encryption, accessible by US-authorized foreign nationals.

Minimally Protected Environment

- Unencrypted networks connected to the Internet or NIPRNET, either directly or via a firewall.

1.3.4.6 General usage

This section contains definitions for five levels of assurance, and guidance for their application. The guidance is based on the previous discussion of information value and environmental protection. Emphasis is placed on two types of activity: integrity and access control to information considered sensitive by the DoD, and information related to electronic financial transactions and other e-commerce. The final selection of the security mechanisms and level of strength and assurance requires a risk management process that addresses the specific mission and environment. The authority responsible for approving a specific level of assurance required for a particular implementation will vary from organization to organization, but will normally be the system accreditor acting in accordance with the applicability guidance that follows.

DoD Class 2: This level is intended for applications handling unclassified information of low value in a Minimally or Moderately Protected Environment. DoD CAs will not issue CLASS 2 certificates; the DoD shall issue CLASS 3 and CLASS 4 certificates exclusively. Access to DoD information resources shall never be allowed on the basis of CLASS 2 certificates. CLASS 2 certificates, (or non-DoD equivalent certificates) may be accepted by DoD relying parties for the purpose of authenticating or encrypting communication that does not access or process DoD information (meeting coordination, accessing web site information that has been cleared for unlimited distribution. etc.) These certificates may, for example, be issued by non-DoD commercial entities.

DoD Class 3: This level is intended for applications handling unclassified medium value information in Moderately Protected Environments, unclassified high value information in Highly Protected Environments, and discretionary access control of classified information in Highly Protected Environments.

Guidance:

- All applications appropriate for CLASS 2 certificates;
- Digital signature services for Mission Assurance Category I (MAC I) and national security information on an encrypted network;
- Privacy and authentication in support of access control security services (e.g., separation of communities of interests) for access to classified Special Compartmented or Special Access information on networks protected using NSA approved Type 1 cryptography appropriate to the data being protected, or on networks that are physically isolated and approved to process the classified data.
- Acceptable non-repudiation for small and medium value financial transactions other than transactions involving issuance or acceptance of contracts and contract modifications. This would include acceptance and payment for small and medium value financial transactions, travel claims, payroll, etc.

DoD Class 3 Hardware: This level is intended for applications handling unclassified medium value information in Minimally Protected Environments, unclassified high value information in Moderately Protected Environments, and discretionary access control of classified information in Highly Protected Environments. This level is also intended for all applications operating in environments appropriate for CLASS 3 but which require a higher degree of assurance and technical non-repudiation.

This level is intended for applications performing contracting and contract modifications.

Guidance:

- All applications appropriate for CLASS 2 or CLASS 3 certificates;
- Note that the requirements for CLASS 3 Hardware are the same as those for CLASS 3 unless otherwise indicated in this CP.

DoD Class 4: This level is intended for applications handling high value unclassified information (Mission Assurance Category I (MAC I), NSSI) in Minimally Protected environments.

Guidance:

- All applications appropriate for CLASS 3 certificates;
- Digital signature services for unclassified Mission Assurance Category I (MAC I) or national security information in an unencrypted network;
- Protection (authentication and confidentiality) for information crossing classification boundaries when such a crossing is already permitted under a system security policy (e.g. sending unclassified information through a HAG from SIPRNET to NIPRNET);
- Technical non-repudiation for large value financial or electronic commerce applications.

DoD Class 5: This level is intended for applications handling classified material in Minimally Protected Environments, and authentication of material that would affect the security of classified systems.

This policy does not currently define the requirements associated with CLASS 5 certificates. As National Manager for National Security Telecommunication and Information Systems Security (NSTISS), only the Director, NSA, may approve the use of a lower assurance certificate to protect classified material in a Minimally Protected Environment. Procedures for issuance and use of specific DIRNSA-approved certificates will be separately documented and referenced in the CPS of the issuing CA.

1.3.4.7 General usage summary

The General Usage is summarized in the following table. The levels of assurance listed are minimums. Any application that requires information to cross a classification boundary requires CLASS 4 level of assurance.

Value of Information	Protection of Network Environment		
	High	Moderate	Minimal
Low	CLASS 3	CLASS 3	CLASS 3
Medium	CLASS 3	CLASS 3	CLASS 3 Hardware
High	CLASS 3	CLASS 3 Hardware	CLASS 4

1.4 CONTACT DETAILS

1.4.1 Specification administration organization

The PMA is responsible for the definition, revision and promulgation of this policy. The PMA is the Office of the Assistant Secretary of Defense for Networks and Information Integration, (OASD/NII), and its designees.

1.4.2 Contact information

Questions regarding this CP should be directed to

DoD PKI PMO
ATTN: V
DEPARTMENT OF DEFENSE
9800 SAVAGE RD STE 6737
FT MEADE MD 20755-6737

1.4.3 Person determining Certification Practice Statement suitability for the policy

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

2 GENERAL PROVISIONS

2.1 OBLIGATIONS

2.1.1 CA obligations

A CA who issues certificates that assert a policy defined in this document shall conform to the stipulations of this document, including:

- providing to the 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 to maintain 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 2.1.3, and informed 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 2.2; and
- operating or providing for the services of an on-line repository that satisfies the obligations under Section 2.1.5, and informing the repository service provider of those obligations if applicable.

A CA who is found to have acted in a manner inconsistent with these obligations is subject to action as described in Section 2.5.5.

2.1.2 RA obligations

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 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. For example, the RA may collect information for the CA only, or it may build the certificate for the CA to sign. CAs are ultimately responsible for ensuring that the 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 requirements, and who agree to abide by them. Security requirements imposed on the CA are likewise imposed on any RAs to the extent that the RAs are responsible for the information collected.

2.1.3 Subscriber obligations

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

PKI Sponsors (as described in Section 5.2.1.4) assume the obligations of Subscribers for the certificates associated with their components.

2.1.4 Relying party obligations

Parties who rely upon the certificates issued under a policy defined in this document shall:

- use the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension);
- check each certificate for validity, using procedures described in the X.509 standard [ISO 9594-8], prior to reliance;
- establish trust in the CA who issued a certificate by verifying the certificate path in accordance with the guidelines set by the X.509 Version 3 Amendment;
- preserve original signed data, the applications necessary to read and process that data, and the cryptographic applications needed to verify the digital signatures on that data for as long as it may be necessary to verify the signature on that data. Note: data format changes associated with application upgrades will often invalidate digital signatures and shall be avoided.

CMAs who verify certificates using Online Certificate Status Protocol (OCSP) shall only use OCSP Responders approved by the PMA.

2.1.5 Repository obligations

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;
- provide access control mechanisms sufficient to protect repository information as described in Section 2.4.3.

2.1.6 OCSP Responder obligations

A OCSP Responder that has been issued a DoD PKI Certificate shall conform to the stipulations of this document including operating under a CPS that has been approved by the PMA. Such OCSP Responders who are found to have acted in a manner inconsistent with these obligations are subject to action as described in Section 2.5.5

All OCSP Responders that provide DoD relying parties with revocation status for certificates that assert a policy defined in this document shall conform to the following:

- Providing to the PMA a CPS, as well as any subsequent changes;
- Conforming to the stipulations of the submitted CPS;
- Ensuring that certificate and revocation information is accepted only from valid DoD approved CAs; and
- Maintain evidence that due diligence was exercised in validating the certificate status.

2.2 REQUIREMENTS FOR ISSUING TO NON-US GOVERNMENT SUBSCRIBERS

DoD CAs may issue certificates to Subscribers other than officers and employees of the US Government, such as contractors, commercial vendors and foreign nationals, for the convenience of the Government and without fee, when those Subscribers have a bona fide need to possess a certificate issued by a DoD CA. DoD CAs shall impose the stipulations of this section upon Subscribers by including the following provisions in the Subscriber agreements.

2.2.1 Liability

A non-US Government Subscriber will have no claim against the DoD arising from use of the Subscriber's certificate or a CMA's determination to terminate a certificate. In no event will the DoD be liable for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to any certificate issued by a DoD CA.

2.2.2 Governing law

This Policy shall be governed by the laws of the United States of America.

2.3 INTERPRETATION AND ENFORCEMENT

2.3.1 Severability of provisions, survival, merger, and notice

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 8. Responsibilities, requirements, and privileges of this document are merged to the newer edition upon release of that newer edition.

2.3.2 Dispute resolution procedures imposed on Subscribers

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

2.4 PUBLICATION AND REPOSITORY

2.4.1 Publication of CA information

Each CA shall provide an on-line repository that is available to Subscribers and relying parties and that contains:

1. issued encryption certificates that assert this Policy;
2. a CRL;
3. the CA's certificate for its certificate signing key; and
4. a copy of this Policy, including any waivers granted to the CA by the PMA.

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 Subscriber duties and responsibilities.

2.4.2 Frequency of publication

Certificates are published following Subscriber acceptance as specified in Section 4.3 and proof of possession of private key as specified in Section 3.1.7. The CRL is published as specified in Section 4.4.3.1. 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.

2.4.3 Access controls

A CA shall protect any repository information not intended for public dissemination or modification.

2.4.4 Repositories

The location of any publication will be one, which provides access to Subscribers and Relying Parties in accordance with the total security requirements.

2.5 COMPLIANCE AUDIT

2.5.1 Frequency of entity compliance audit

All CAs and Centralized OCSP Responders shall be audited on an annual basis, except for the Certificate Authority Workstations (CAW)-based infrastructure, which shall be audited on a biennial basis. The Services or Agencies shall also have the right to require periodic and aperiodic inspections of OCSP Responder operations to validate that the OCSP Responder is operating in accordance with the security practices and procedures described in its CPS. Additionally, all CAs have the right to require periodic and aperiodic inspections of subordinate CMA operations to validate that the subordinate CMA is operating in accordance with the security practices and procedures described in the subordinate's CPS. The CA will state the reason for any aperiodic inspection.

The PMA has the right to require aperiodic compliance audits of CMAs asserting this policy. The PMA shall state the reason for any aperiodic compliance audit.

2.5.2 Identity/qualifications of compliance auditor

The auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with the CMA's CPS. The compliance auditor must perform CA or Information System compliance audits as a primary responsibility. The CPS shall name the compliance auditor for each CMA.

2.5.3 Compliance auditor's relationship to audited party

The compliance auditor and CA and OCSP Responders shall have a contractual relationship for the performance of the compliance audit, or be sufficiently organizationally separated from the audited CA or OCSP Responders to provide an unbiased, independent evaluation.

2.5.4 Topics covered by compliance audit

The purpose of a compliance audit shall be to verify that the CA and OCSP Responder have in place a system to assure the quality of the CA or OCSP Responder services that it provides, and that it complies with all of the requirements of this CP and its CPS. All aspects of the CA or OCSP Responder operation related to this CP shall be subject to compliance audit inspections.

2.5.5 Actions taken as a result of deficiency

When the compliance auditor finds a discrepancy between a CMA's operation and the stipulations of its CPS, the following actions must occur:

- the compliance auditor shall note the discrepancy;
- the compliance auditor shall notify the parties identified in Section 2.5.6 of the discrepancy;
- the CA will propose a remedy, including expected time for completion, to the DoD PKI Program Management Office (PMO).

If the compliance auditor finds a critical failure that contributes to the ongoing compromise of sensitive information, the compliance auditor shall immediately report the issue to both the local authority (local base commander or Information System Security Officer (ISSO)) and the PMA Director, DoD PKI PMO Certificate Policy Management Working Group (CPMWG) to determine if the circumstances warrant the immediate shut down of operations, and/or the revocation of associated certificates. Such failures could include, but are not limited to: detection of a successful attempt to compromise sensitive information; detection of an overt and intentional disregard for secure operations of the system, detection of a system configuration that causes the wide-spread public dissemination of sensitive information.

The PMA will determine the appropriate remedy, up to and including revocation or non-recognition of the certificate of the CMAA. Upon correction of the deficiency, the PMA may reinstate the CMA.

2.5.6 Communication of results

.

The compliance auditor shall report the results of a CMA compliance audit to the PMA. The results will be reported to the audited CMA, and its superior CA if applicable, in accordance with Section 2.6. The implementation of remedies shall be communicated to the PMA. The PMA as the authorized party will determine the appropriateness of the remedy and may take additional measures as defined in Section 2.5.5. A special compliance audit may be required to confirm the implementation and effectiveness of the remedy

2.6 CONFIDENTIALITY

2.6.1 Types of information to be protected

A certificate should only contain information that is relevant and necessary to effect secure transactions with the certificate. For the purpose of proper administration of the certificates, a CMA may request non-certificate information to be used in managing the certificates within an organization (e.g., identifying numbers, business or home addresses and telephone numbers). Any such information shall be explicitly identified in a CPS. All information stored locally on the CA equipment and not in the repository shall be handled as sensitive, and access shall be restricted to those with an official need-to-know in order to perform their official duties or in accordance with Section 2.6.2.

2.6.2 Information Release Circumstances

A CA will not disclose certificate or certificate-related information to any third party unless authorized by this Policy, required by law, government rule or regulation, or order of a court of competent jurisdiction. Any request for release of information shall be authenticated.

2.7 INTELLECTUAL PROPERTY RIGHTS

The US DoD shall maintain ownership of any public key certificates and private keys that it issues.

3 IDENTIFICATION AND AUTHENTICATION

3.1 INITIAL REGISTRATION

3.1.1 Types of names

All CAs shall be able to generate and sign certificates that contain an X.500 Distinguished Name (DN). Certificates issued to CAs and RAs shall use the DN form, as shall **CLASS 4** assurance certificates.

In general, CAs shall not assign DNs. Subscribers shall have DNs assigned to them through their organizations, in accordance with a naming authority (see Section 3.1.2). Some certificates may additionally assert an alternate name form. Details related to this requirement are provided in Section 7.1.4.

CLASS 2	Non-null Subject Name with optional SubjectAlternativeName if marked non-critical, or Null Subject Name if Subject Alternative Name is populated and marked critical
CLASS 3, CLASS 4	Non-null Subject Name, and optional Subject Alternative Name if marked non-critical

3.1.2 Need for names to be meaningful

Names used within the DoD shall identify the person or object 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 for humans. For people, this will typically be a legal name. For equipment, this may be a model name and serial number, or an application process (e.g., *Organization X Mail List* or *Organization Y Multifunction Interpreter*).

The DoD will establish one or more authorities for the creation of DNs. A CMA who uses DNs will coordinate with such an authority to determine the proper elements for a given Subscriber.

Each root CA asserting this policy shall only sign certificates with subject names from within a name-space approved by the 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 Rules for interpreting various name forms

Rules for interpreting name forms are contained in the applicable certificate profile (see Section 7.1.2), and are established by a naming authority if one exists, or by the CA itself. The naming authority shall be identified contractually or in a CPS.

3.1.4 Uniqueness of names

Name uniqueness across the DoD must be enforced. Wherever practical, X.500 DNs allocated from a DoD naming authority shall be used, and the CAs and RAs shall enforce name uniqueness within the X.500 name space, which they have been authorized. When other name forms are used, they too must be allocated such that name uniqueness across the DoD is ensured. A CA shall document in its CPS what name forms will be used, how the CA and RAs will interact with DoD naming authorities, and how they will allocate names within the Subscriber community to guarantee name uniqueness among current and past Subscribers (i.e., if “Joe Smith” leaves a CA’s community of Subscribers, and a new, different “Joe Smith” enters the community of Subscribers, how will these two people be provided unique names).

3.1.5 Name claim dispute resolution procedure

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.

3.1.6 Recognition, authentication, and role of trademarks

A corporate entity is not guaranteed that its name will contain a trademark if requested. The CMA shall not knowingly issue a certificate including a name that a court of competent jurisdiction has determined infringes the trademark of another. It is not subsequently required to issue that name to the rightful owner if it has already issued one sufficient for identification within the DoD. A CMA shall not be obligated to research trademarks or resolve trademark disputes.

3.1.7 Method to prove possession of private key

In all cases where the Subscriber generates keys, the Subscriber shall be required to prove, to the CMA, possession of the private key, which corresponds to the public key in the certificate request. For signature keys, this may be done by signing the request. For key management keys, the CA or RA may encrypt the Subscriber's certificate in a confirmation request message. The Subscriber can then decrypt and return the certificate to the CA or RA in a confirmation message. The PMA may determine other mechanisms that are at least as secure as those cited here to be acceptable.

In the case where key is generated directly on the Subscriber's token, or in a key generator that benignly transfers the key to the Subscriber's token, then the Subscriber is in possession of the private key at the time of generation or transfer. If the Subscriber is not in possession of the token when the key is generated, then the token shall be delivered to the Subscriber via an accountable method (see Section 6.1.2).

For all assurance levels, when keyed hardware tokens are delivered to Subscribers, the delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers. The CMA must maintain a record of validation for receipt of the token by the Subscriber. When any mechanism that includes a shared secret (e.g., a password or pin) is used, the mechanism shall ensure that the applicant and the CMA are the only recipients of this shared secret.

3.1.8 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 and these CMAs shall preclude the use of organization certificates where individual non-repudiation is required.

3.1.9 Authentication of individual identity

3.1.9.1 In-Person Authentication

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. Additionally a CMA shall record the process that was followed for each certificate. 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
- the date of the verification.

Additionally, the process documentation must include a declaration of identity. The declaration shall be signed with a handwritten signature or, if a good fingerprint or other adequate biometric is collected and can be linked to the subscriber identity, a digital signature. Either signature must be applied in the presence of the person performing the identity authentication.

For CLASS 2, the basis of establishing identity is through an association with a service, agency, or other component of the DoD. Examples of mechanisms that establish this association are: an applicant or supervisor's request via official communication mechanism (internal mail), a DoD-wide database, or a system account.

For CLASS 3 and CLASS 4, applicant identity proofing requires the applicants to provide at least one federal government official picture identification credential (such as a DoD identification card or passport), or two non-federal government issued official identification credentials, at least one of which must be a photo ID, such as a drivers license. 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 CLASS 3, the applicant's identity must be personally verified prior to the applicant's certificate being enabled. The applicant shall appear personally before either:

- A CMA;
- A Trusted Agent personally approved by the CMA or appointed by name in writing to the CMA by the Commanding Officer/Officer in Charge of the organization which they represent, or;
- A person certified by a State or Federal Government as being authorized to confirm identities (such as Notaries Public), that uses a stamp, seal, or other mechanism to authenticate their identity confirmation.

The applicant shall appear before one of the required identity verifiers no more than 30 days prior to application of the CA's signature to the applicant's certificate, or alternatively, when private keys are delivered to Subscribers via hardware tokens, the Subscribers shall personally appear before the CMA or CMA's Trusted Agent to obtain their tokens or token activation data.

FOR CLASS 3 HARDWARE or CLASS 4, the applicant's identity shall be personally verified by a CMA prior to the applicant's certificate being enabled. There are two ways to meet this requirement:

- The applicant shall personally appear before the CMA, or a Trusted Agent personally approved by the CMA or appointed by name in writing to the CMA by the Commanding Officer/Officer in Charge of the organization which they represent, at any time prior to application of the CA's signature to the applicant's certificate, or
- When private keys are delivered to Subscribers via hardware tokens, the Subscribers shall personally appear before the CMA to obtain their tokens or token activation data.

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.

CLASS 2	Identity may be established by database, supervisor, or Subscriber
CLASS 3	Must appear in person to Trusted Agent, Notary (or equivalent), or CMA, and present official picture ID
CLASS 3 HARDWARE or CLASS 4	Must appear in person to CMA or Trusted Agent, and present official picture ID

3.1.9.2 Electronic Authentication

CLASS 2, CLASS 3, CLASS 3 Hardware or CLASS 4 certificates may be issued on the basis of electronically authenticated (using a current, valid DoD PKI signature certificate and associated private key) Subscriber requests, subject to the following restrictions:

- The assurance class of the new certificate shall be the same or lower than the assurance class 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.

Electronically authenticated issuance is similar to certificate re-key (section 3.2.1) except that the new certificate is valid concurrently with the existing certificate but with a potentially different expiration date

3.1.10 Authentication of Component Identities

Some computing and communications components (routers, firewalls, etc.) will be named as certificate subjects. In such cases, the component must have a human PKI Sponsor as described in Section 5.2.1.4. The PKI Sponsor is responsible for providing the CMA, or to CMA approved Trusted Agents as described in Sections 3.1.9 and 5.2.1.4, correct information regarding:

- equipment identification
- equipment public keys
- equipment authorizations and attributes (if any are to be included in the certificate)
- contact information to enable the CMA to communicate with the PKI sponsor when required.

The CMA, or their Trusted Agents, shall authenticate the validity of any authorizations to be asserted in the certificate, and shall verify source and integrity of the data collected to an assurance level commensurate with the certificate CLASS being requested. Acceptable methods for performing this authentication and integrity checking include, but are not limited to:

- Verification of digitally signed messages sent from PKI sponsors (using certificates of equivalent or greater assurance than that being requested).
- In person registration by the PKI Sponsor, with the identity of the PKI Sponsor confirmed in accordance with the requirements of Section 3.1.9.

3.2 CERTIFICATE RENEWAL, UPDATE, AND ROUTINE RE-KEY

3.2.1 Certificate re-key

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 its identity. Re-keying a certificate means that a new certificate is created that is identical to the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key); a different serial number; and may be assigned a different validity period.

Re-key requests for CLASS 2 or CLASS 3 (excluding CLASS 3 Hardware) certificates can be authenticated on the basis of existing Subscriber certificates twice, after which the Subscriber must identify itself as for a new request, in accordance with Section 3.1. Registration as for a new request is periodically required to limit the damage caused by unreported key compromises. For example, a CLASS 3 assurance certificate Subscriber may identify itself in-person, then request re-key authenticating using its existing certificate in year three, and again in year six. In year nine, the Subscriber must request a new certificate in person. Applications for re-key using existing certificates shall result in new certificates asserting the same level of assurance as that asserted in the old certificate that was used to authenticate the re-key request.

CLASS 3 HARDWARE or CLASS 4 assurance certificates may be renewed or updated on the basis of electronically authenticated Subscriber requests. Every three years, in-person authentication is required, in accordance with Section 3.1.

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.

The key lifetimes given are maximums. A program may always require shorter lifetimes. The following key lifetimes are for Subscribers; CA key lifetimes are provided in Section 4.7.

CLASS 2	Signature re-key every five years Confidentiality re-key every five years Identity established through use of current signature key Must prove possession of corresponding private key May authenticate to PKI for rekey with current key twice
CLASS 3	Signature re-key every three years Confidentiality re-key every three years Identity established through use of current signature key Must prove possession of corresponding private key May authenticate to PKI for rekey with current key twice
CLASS 3 HARDWARE or CLASS 4	Signature re-key every three years Confidentiality re-key every three years Identity established in person Must prove possession of corresponding private key

3.2.2 Certificate renewal

Renewing a certificate means creating a new certificate with the same name, key, and authorizations as the old one, but a new, extended validity period and a new serial number. Certificates may be renewed as a means of CRL size management. A certificate may be renewed if the public key has not reached the end of its validity, the associated private key has not been compromised, and the Subscriber name and attributes are correct. Thus, a CMA may choose to implement a three-year rekey period with an initial issue and two annual renewals. The old certificate need not be revoked, but must not be further rekeyed, renewed, or updated.

3.2.3 Certificate update

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. For example, a CA may choose to update a certificate of a Subscriber who gains an authorization. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or updated.

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.

3.3 OBTAINING A NEW CERTIFICATE AFTER REVOCATION

For all levels of assurance, Subscribers requesting certificates after revocation must meet initial registration requirements.

3.4 REVOCATION REQUEST

Revocation requests must be authenticated; see Section 4.4.1.3. 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.

4 OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

It is the intent of this Policy to identify the minimum requirements and procedures that are necessary to support trust in the PKI, and to minimize imposition of specific implementation requirements on CMAs, Subscribers, and relying parties.

The applicant and the CMA must perform the following steps when an applicant applies for a certificate:

- establish and record identity of Subscriber (per Section 3.1);
- obtain a public/private key pair for each certificate required;
- establish that the public key forms a functioning key pair with the private key held by the Subscriber (per Section 3.1.7);
- provide a point of contact for verification of any roles or authorizations requested.

These 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 issuance. All communications among CMAs supporting the certificate application and issuance process 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 CLASS 3 certificates shall be protected using CLASS 3 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.

CAs implementing this CP shall certify other CAs (to include cross-certification) only as authorized by the DoD PMA.

Requests by CAs for CA certificates shall be submitted to the DoD PMA using the contact provided in Section 1.4, and shall be accompanied by a CPS written to the format of the *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* [RFC2527].

The DoD PMA will evaluate the submitted CPS for acceptability. The PMA may require an initial compliance audit, performed by parties of the PMA's choosing, to ensure that the CMA is prepared to implement all aspects of the submitted CPS, prior to the DoD PMA authorizing the CMA to issue and manage certificates asserting the DoD CPs.

CAs shall only issue certificates asserting DoD CPs upon receipt of written authorization from the DoD PMA, and then may only do so within the constraints imposed by the PMA or its designated representatives.

4.1.1 Delivery of Subscriber's public key 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 stipulated in the CPS.

In those cases where public/private key pairs are generated by the CMA on behalf of the Subscriber, the CMA shall implement secure mechanisms to ensure that the token on which the public/private key pair is held is securely sent to the proper Subscriber, and that the token is not activated prior to receipt by the proper Subscriber.

4.2 CERTIFICATE ISSUANCE

Upon receiving the request, the CMA will:

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

- build and sign a certificate, if all certificate requirements have been met (in the case of an RA, have the CA sign the certificate); and
- make the certificate available to the Subscriber.

The certificate request may contain an already built ("to-be-signed") certificate. This certificate will not be signed until all verifications and modifications, if any, have been completed to the CA's satisfaction. If a certificate request is denied, then the CA will not sign the requested certificate, and will work with the RA to resolve the problem.

While the Subscriber may do most of the data entry, it is still the responsibility of the CMA to verify that the information is correct and accurate. This may be accomplished either through a system approach linking databases containing personnel information or through personal contact with the program's attribute authority (as put forth in the CMA's CPS). If databases or other sources are used to confirm Subscriber attributes, then these sources and associated information sent to a CMA must be protected from unauthorized modification to a level commensurate with the level of assurance specified for the certificates conveying the Subscriber attributes. EXCEPTION: Class 3 hardware certificates may be used until 01 January 2006 to confirm CLASS 4 Subscriber attributes.

CMAs shall verify all authorization and other attribute information received from an applicant. In most cases, the RA is responsible for verifying applicant data, but if CAs accept applicant data directly from applicants, then the CA is responsible for verifying the applicant data. 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.

4.2.1 Delivery of Subscriber's private key to Subscriber

In most cases, a private key will be generated and remain within the cryptographic boundary of a cryptographic module. If the owner of the module generates the key locally, then there is no need to deliver the subscriber's private key. If the key is generated on a hardware cryptographic module elsewhere, then the hardware cryptographic module must be delivered to the Subscriber. Accountability for the location and state of the hardware cryptographic module must be maintained until the Subscriber is in possession of it. The Subscriber shall acknowledge receipt of the hardware cryptographic module.

Private keys associated with CLASS 2 and CLASS 3 (excluding CLASS 3 Hardware) certificates may be generated and stored in software cryptographic modules. When the Subscriber generates these keys locally, there is no need to deliver them. If the private keys are generated elsewhere, they must be transmitted or delivered to the subscriber in encrypted form and the encryption method ensures that only the subscriber may possess the plaintext private signature keys. The encryption must be of strength commensurate with that of the key being protected. The subscriber shall acknowledge receipt of the private signature key. The originally generated private signature key shall be destroyed. Mechanisms shall ensure that additional copies of software keys are not maintained except as allowed in this Certificate Policy.

Only those authorized by the DoD key recovery policy may access private keys associated with encryption certificates.

Public-key certificates shall be issued in the name of an individual whenever possible, and the private keys associated with such certificates shall never be shared with any other person. For those cases where there must be several persons acting in one role or in a group, a certificate may be issued 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 highly preferred 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. Certificates corresponding to private keys held by multiple Subscribers shall not be used for contracting or e-commerce applications).

A local authority shall authorize the creation of group or role certificates. In these cases:

- the group/role 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 Sponsor shall forward an initial list and periodically forward all updates since the last submission of this list to the local ISSO.

- the ISSO is responsible for periodically reviewing the Sponsor's list with an eye towards identification of anomalies.

- a list of those holding the shared private key will be made available to the CA and RA, upon request.

The procedures for issuing tokens for use in shared key applications must comply with all other stipulations of this Policy (e.g., key generation, private key protection, Subscriber obligations, etc.).

4.2.2 CA public key delivery to users

The PKI and the relying parties must work together to ensure the authenticated and integral delivery of Trusted 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 certificate hashes or fingerprints against Trusted Certificate hashes or fingerprints made available via authenticated out-of-band sources (note that fingerprints or hashes posted in-band along with the certificate are not acceptable as an authentication mechanism); and
- loading certificates from web sites secured with a currently valid DoD certificate of equal or greater assurance level than the certificate being downloaded.

Systems using Class 4 certificates shall store Trusted Certificates such that unauthorized alteration or replacement is readily detectable.

4.3 CERTIFICATE ACCEPTANCE

Before a CA allows a Subscriber to make effective use of its private key, a CMA shall

- explain to the Subscriber its responsibilities as defined in Section 2.1.3;
- inform the Subscriber of the creation of a certificate and the contents of the certificate;
- require the Subscriber to indicate acceptance of its obligations and its certificate, with either a digital or handwritten signature; and
- document the Subscriber's acceptance of its responsibilities and its certificate.

The ordering of this process, and the mechanisms used, will depend on factors such as where the key is generated and how certificates are posted. In the case of non-human components (router, firewalls, etc.), the PKI Sponsor (as defined in Section 5.2.1.4) shall perform the functions of the Subscriber.

4.4 CERTIFICATE SUSPENSION AND REVOCATION

4.4.1 Revocation

4.4.1.1 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. Examples of circumstances that invalidate the binding are:

- identifying information or affiliation components of any names in the certificate become invalid;
- 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;
- the Subscriber or other authorized party (as defined in the CMA's CPS) asks for his/her certificate to be revoked.

Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on the CRL. In addition, 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.

4.4.1.2 Who can request a revocation

Within the PKI, a CMA may summarily revoke certificates within its domain. A written notice and brief explanation for the revocation shall subsequently be provided to the Subscriber. The RA can request the revocation of a Subscriber's certificate on behalf of any authorized party as specified in its CPS.

4.4.1.3 Procedure for revocation request

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). A CMA action is required for revocation (a Subscriber may not, via an automated process, revoke its own certificate or change a prior revocation reason without CMA intervention). Authentication of certificate revocation requests is important to prevent malicious revocation of certificates by unauthorized parties.

In particular, if the revocation is being requested for 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, a formal, signed message format known to the CA shall be employed. All requests shall be authenticated; for signed requests from the certificate subject, or from a RA, verification of the signature is sufficient.

Upon receipt of a revocation request from the Subscriber or another authorized party, the CMA 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 by placing its serial number and other identifying information on a CRL, in addition to any other revocation mechanisms used.

For PKI implementations using hardware tokens, Subscribers leaving organizations that sponsored their participation in the PKI shall surrender to their CMA (through any accountable mechanism) all cryptographic hardware tokens that were issued under the sponsoring organization 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. If a Subscriber leaves an organization and the hardware tokens cannot be obtained from the Subscriber, then all Subscribers' certificates associated with the unretrieved tokens shall be revoked.

4.4.1.4 Revocation grace period

There is no grace period for revocation under this policy; CAs will revoke certificates as quickly as practical upon receipt of a proper revocation request, and shall always revoke certificates within the time constraints described in Section 4.4.3.1.

4.4.2 Suspension

Certificates that are issued under this Policy, and that are placed on a CRL, shall not subsequently be considered valid (e.g., by removing them from a subsequent CRL).

4.4.3 Certificate Revocation Lists

4.4.3.1 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 superceded CRLs are removed from the repository upon posting of the latest CRL.

The DoD CAs shall conform to the CRL issuance frequency described in the table below

	Normal CRL Issuance Periodicity	**Maximum CRL Issuance Latency for the reason of key or CA compromise**
CLASS 2 CA	No required period	Within 24 hours of notification
CLASS 3, 3H Root CA	At least once every 28 days	Within 18 hours of notification
CLASS 3, 3H Signing CA	At least one each day	Within 18 hours of notification
CLASS 4 Root CA	At least once every 28 days	Within 6 hours of notification
CLASS 4 Signing CA	At least once each day	Within 6 hours of notification
NSM PAA, PCA, CA	At least once eve ry 28 days	Within 6 hours of notification

CLASS 4 assurance Subscriber certificates, when revoked for reason of key compromise, shall be listed on an Indirect Certificate Revocation List (ICRL), in accordance with [SDN706], or some mechanism of equivalent functionality and timeliness, within six hours of receipt of the revocation request by an infrastructure component (RA or CA). A CLASS 4 CA certificate, revoked for any reason, shall also be placed on the CLASS 4 ICRL in accordance with [SDN706], or some mechanism of equivalent functionality and timeliness, within six hours of receipt of the revocation request.

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.

The DoD Root CA shall immediately notify any externally certified CAs in the event of a subordinate CA revocation for any reason.

4.4.3.2 CRL checking requirements

Use of revoked certificates could have damaging or catastrophic consequences in certain applications. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party and the system accreditor. If it is temporarily infeasible to obtain revocation information, then the Relying Party must either reject use of the certificate, or make an informed decision to accept the risk, responsibility, and

consequences for using a certificate whose authenticity cannot be guaranteed to the standards of this policy. Such use may occasionally be necessary to meet urgent operational requirements.

4.4.4 On-line status checking

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.

DoD relying parties shall only rely upon OCSP Responders approved by the DoD PMA as meeting the requirements of section 2.1.6.

OCSP Responders shall ensure that:

- Accurate and up-to-date information from the authorized CA is used to provide the revocation status; and
- Revocation status responses provide authentication and integrity services commensurate with the assurance level of the certificate being checked.

4.4.5 Other forms of revocation advertisements available

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

- The alternative method must be described in the CA's approved CPS;
- The alternative method must provide authentication and integrity services commensurate with the assurance level of the certificate being verified.

4.4.6 Special requirements related to key compromise

A CMA using reason codes must have the ability to transition any reason code to compromise. Operational stipulations are in Section 4.4.3. Refer also to Sections 4.8.1 and 5.3.6.

4.5 SECURITY AUDIT PROCEDURES

This section describes the security requirements of a CMA's certificate issuing system, which includes the equipment used to register Subscribers; generate, sign, and manage certificates; and generate, sign, and manage revocation information.

4.5.1 Types of events recorded

For CLASS 2, certificate issuance and revocation shall be recorded.

Requirements applied to CLASS 3 and CLASS 4 CA, OCSP Responder and RA equipment:

Any security auditing capabilities of the underlying CMA equipment operating system shall be enabled during installation.

At a minimum, the following CMA events shall be recorded:

- CMA application access (e.g., logon);
- messages received from any source requesting CMA actions, (certificate requests, certificate signing, certificate revocation, compromise notification); OCSP Responders are exempt from this audit requirement.
- actions taken in response to requests for CMA actions; for OCSP Responders, the audit function shall intermittently be configured to collect a sample of responses sent. At a minimum an average of 10% of the responses shall be collected per workday.
- physical access to, loading, zeroizing, transferring keys to or from, backing-up, acquiring or destroying CMA cryptographic modules;
- receipt, servicing (e.g., keying or other cryptologic manipulations), and shipping hardware cryptographic modules;
- posting of any material to a repository;

- anomalies, error conditions, software integrity check failures, receipt of improper or misrouted messages; and
- 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.

Requirements applied to CLASS 3 and CLASS 4 CA equipment and Centralized OCSP Responders:.

The CA equipment and Centralized OCSP Responders shall record server installation, access, and modification (to include changes in configuration files, security profiles, administrator privileges).

For CLASS 3 and CLASS 4, the following operations must be recorded for CAs and Centralized OCSP Responders:

- CA equipment and Centralized OCSP Responders access (e.g., room access)
- file manipulation and account management
- posting of any material to a repository.
- access to CA databases and Centralized OCSP Responder databases.
- any use of the CA or Centralized OCSP Responders signing key

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

- the type of event
- the time the event occurred
- for messages from RAs (or other entities) requesting CA actions, the message source, destination and contents
- for attempted CA certificate signature or revocation – a success or failure indication
- for operator initiated actions (including equipment and application access), the identity of the equipment operator who initiated the action.

Where possible, the security audit data shall be automatically collected; when this is not possible a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained in accordance with the requirements of Section 4.5.3, and made available during compliance audits.

4.5.2 Frequency of processing data

For Class 2, security audit data review is only required for cause.

For Class 3, at least 6 aperiodic reviews are required per year, with a minimum of 25 percent of the security audit data generated since the last review to be examined.

For Class 4, at least 12 (monthly) reviews are required per year, with at least 33 percent of the security audit data generated since the last review to be examined.

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.

4.5.3 Retention period for security audit data

The information generated on the CMA equipment shall be kept on the CMA equipment until the information is moved to an appropriate archive facility. Deletion of the security audit data from the CMA equipment shall be performed by an entity other than the CMA. This entity shall be identified in the CMA's CPS. Security audit data shall be available on-site for at least two months or until reviewed, then off-site as archive records in accordance with Section 4.6.2.

4.5.4 Protection of security audit data

For CLASS 3 and CLASS 4, the security audit data shall not be open for reading or modification by any human, or by any automated process other than those that perform security audit processing. CMA system configuration and procedures must be implemented together to ensure that only authorized people archive or delete security audit data. The entity performing security audit data archive need not have modify access, but procedures must be implemented to protect archived data from deletion or destruction prior to the end of the security audit data retention period (note that deletion requires modification access). Security audit data shall be moved to a safe, secure storage location separate from the CMA equipment.

4.5.5 Security audit data backup procedures

Security audit data shall be backed up at least monthly. A copy of the security audit data shall be sent off-site on a monthly basis as specified in the CPS.

4.5.6 Security audit collection system (internal vs. external)

The security audit process shall run independently and shall not in any way be under the control of the CMA. Security audit processes shall be invoked at system startup, and cease only at system 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. These mechanisms shall be described in the CMA's CPS.

4.5.7 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.

4.5.8 Vulnerability assessments

The CMA, system administrator, and other operating personnel shall be watchful for attempts to violate the integrity of the certificate management system, including the equipment, physical location, and personnel. The security audit data shall be reviewed by the security auditor for events such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses. Security auditors shall check for continuity of the security audit data.

4.6 RECORDS ARCHIVAL

4.6.1 Types of data archived

CMA archive records shall be detailed enough to establish the validity of a signature and of the proper operation of the PKI. At a minimum, the following data shall be archived.

During CMA system initialization:

For all assurance levels:

- CMA accreditation (if necessary),
- CPSs, and
- any contractual agreements to which the CMA is bound.

Additionally, for CLASS 3 and CLASS 4:

- system equipment configuration.

During CMA operation:

For CLASS 3 and CLASS 4:

- modifications or updates to any of the above data items;

- certificate requests and revocation requests;
- Subscriber identity authentication documentation as required by Section 3.1.9;
- documentation of receipt and acceptance of certificates as described in Section 4.3;
- documentation of receipt of tokens as described in Section 3.1.7;
- all certificates and CRLs (or other revocation information) as issued or published;
- security audit data (in accordance with Section 4.5);
- other data or applications sufficient to verify archive contents
- all work related communications to or from the PMA, other CMAs, and compliance auditors.

4.6.2 Retention period for archive

Archive records shall be kept, without any loss of data, for a period of

- at least seven years, six months for CLASS 2;
- at least ten years, six months for CLASS 3; and
- at least twenty years, six months for CLASS 4;

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

Prior to the end of the archive retention period, the CMA shall provide archived data and the applications necessary to read the archives to a PMA approved DoD archival facility, which shall retain the applications necessary to read this archived data.

4.6.3 Protection of archive

No unauthorized CMA equipment operator shall be able to modify or delete the archive, but archived records may be moved to another medium. If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site. No transfer of medium shall invalidate CMA applied signatures. The CMA shall maintain a list of people authorized to modify or delete the archive, and make this list available during CP compliance audits. Release of sensitive archive information will be as described in Section 2.6.

Archive media shall be stored in a separate, safe, secure storage facility. Prior to archive, archive records shall be labeled with the CMA's distinguished name, the date, and the classification.

4.6.4 Archive backup procedures

No stipulation.

4.6.5 Archive collection system (internal vs. external)

Archive data may be collected in any expedient manner.

4.6.6 Procedures to obtain archive information

Procedures detailing how to create, package, and send the archive information shall be published in a CMA procedures handbook or CPS. Only authorized CMA equipment operators will be allowed to access the archive.

4.7 CA KEY CHANGEOVER

A CA uses a signing (private) key for creating certificates; however, relying parties employ the CA certificate for the life of the Subscriber certificate beyond that signing. Therefore, CAs must not issue Subscriber certificates that extend beyond the expiration dates of their own certificates and public keys, and the CA certificate validity period must extend one Subscriber certificate validity period (listed in Section 3.2) past the last use of the CA private key. To minimize risk to the PKI through compromise of a CAs key, the private signing key will be changed more frequently, and only the new key will be used for certificate signing purposes from that time. The older, but still valid, certificate will be available to verify old signatures until all of the Subscriber certificates signed under it have also expired. If the old private key is used to sign CRLs that contain certificates signed with that key, then the old key must be retained and protected. For a thorough discussion of key changeover, see *Certificate Management Protocol* [RFC2510].

The following table summarizes the maximum validity period of the CA's signature certificate, and the maximum lifetime of the associated authority-signing key (used for certificate signature), separated by a slash. RA key lifetimes are as described for Subscribers in Section 3.2. If a CA certificate and key lifetime are selected that are shorter than a Subscriber's, then the RA certificate and key lifetime shall be no longer than that of the CA. Note that signature keys that have expired for the purposes of certificate signature may still be used for CRL signature. All values are in years.

	CA	Intermediate CA	Root-CA
CLASS 2	10/5	20/10	70/50
CLASS 3	6/3	11/5	36/25
CLASS 4	6/3	11/5	36/25

4.8 COMPROMISE AND DISASTER RECOVERY

4.8.1 Compromise recovery

In case of a CA key compromise, a superior CA shall revoke that CA's certificate, and the revocation information shall be published immediately in the most expeditious manner. Subsequently, the CA installation shall be re-established. If the CA is a Root-CA, the trusted self-signed certificate must be removed from each Relying Party application, and a new one distributed via secure out-of-band mechanisms. Root-CAs shall describe their approaches to reacting to a Root-CA key compromise in their CPSs.

In case of an OCSP Responder key compromise, a CA that issued the OCSP Responder a certificate, shall revoke that OCSP Responder s certificate, and the revocation information shall be published immediately in the most expeditious manner. Subsequently, the OCSP Responder shall be re-keyed.

4.8.2 Disaster recovery

Class 3 and Class 4 CAs are required to maintain a Designated Approving Authority (DAA) approved Disaster Recovery Plan.

In the case of a disaster in which the CA 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 prior to the shorter of the next update field in the latest CRL issued by the CA or one week, then the CA must report to the PMA. The PMA, shall decide whether to declare the CA private signing key as compromised, and reestablish the CA keys and certificates, all cross-certificates, and all subscriber certificates, or 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 that its certificates be revoked. The CA installation shall then be completely rebuilt, by reestablishing the CA equipment, generating new private and public keys, being re-certified, and re-issuing all cross certificates. Finally, all Subscriber certificates shall be re-issued. In such events, any Relying Parties who continue to use certificates signed with the destroyed private key do so at their own risk and the risk of others to whom they forward data.

4.9 CA TERMINATION

CA termination will be handled in accordance with Section 4.8 above. If the termination is for convenience, contract expiration, re-organization, or other non-security related reason, and provisions have been made to continue compromise recovery (including destruction or continued protection of signing key), compliance and security audit, archive, and data recovery services, then neither the terminated CAs certificate, nor certificates signed by that CA, need to be revoked.

If provisions for maintaining these services cannot be made, then the CA termination will be handled as a CA compromise in accordance with Section 4.8.1 above.

Prior to CA termination, CAs shall provide archived data to a PMA approved DoD archival facility.

5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 PHYSICAL CONTROLS

The CA and OCSP Responders shall consist of equipment dedicated to these CMA functions. It shall not perform non-CMA related functions.

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

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.

See [NS4005] for protecting classified information.

5.1.2 Physical access

CA and OCSP Responder equipment shall always be protected from unauthorized access.

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. For example, RA equipment in facilities with controlled access occupied by those holding Top Secret security clearances will not require an additional layer of controlled access surrounding inactivated RA equipment. RA equipment in less secure environments will require additional protection commensurate with the level of risk.

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.

A security check to 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 are responsible, a log identifying the person performing a check at each instance shall be maintained. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated.

For CLASS 2, a security check to the facility housing CA and OCSP Responder equipment shall occur at least once every four days.

Facilities housing CLASS 3 or CLASS 4 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.

Current NSA policy requires that a 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, it must be stored in a container approved for classified cryptographic storage, where access is allowed only to authorized CMA operators as defined in Section 5.2.

5.1.3 Power and air conditioning (Environmental Controls)

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

The CA equipment shall have or be provided with sufficient back-up 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 equipment to cease functioning. Subscribers or Relying Parties with needs for long operation hours or short response times may contract with a CA for additional requirements for backup power.

5.1.4 Water exposures

CA 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. CA operators who have sprinklers for fire control shall have a contingency plan for recovery should the sprinklers malfunction, or cause water damage outside of the fire area.

5.1.5 Fire prevention and protection

A description of the CMA's approach for recovery from a fire disaster shall be included in the Disaster Recovery Plan required by Section 4.8.2

5.1.6 Media storage

Media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic). Media that contains security audit, archive, or backup information shall be stored in a location separate from the CMA equipment.

5.1.7 Waste disposal

Normal office waste shall be removed or destroyed in accordance with local policy. Media used to collect or transmit information discussed in Section 2.6 shall be destroyed, such that the information is unrecoverable, prior to disposal.

5.1.8 Off-site backup

System backups, sufficient to recover from system failure, shall be made on a periodic schedule. For CLASS 3 and CLASS 4 CAs that are continuously operated (for periods of one week or longer), full system backups shall be performed once a week. For intermittently operated CLASS 3 and CLASS 4 CAs, the full system backup shall be performed each time the system is turned on or once a week, whichever is less frequent. At least one backup copy shall be stored at an offsite location (separate from the CA equipment). Only the latest backup need be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational CA system.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be diligent and trustworthy as described in the next section. The functions performed in these roles form the basis of trust in the entire PKI. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first approach is to ensure that the person filling the role is trustworthy and properly trained. The second is to distribute the functions of the role among several people, so that any malicious activity requires collusion.

Requirements regarding the design and configuration of the technology to avoid mistakes and counter inappropriate behavior are described in Section 6.

The primary trusted roles defined by this policy are the CA, the OCSP Responder, and the RA.

5.2.1.1 Certification Authority

All certificates asserting a DoD certificate policy must be issued by a CA facility operating under the control of a CA. The responsible person or body (e.g., board of directors) identified as the facility's CA must be named, and made available during compliance audits.

Any CA who asserts a policy identifier defined in this document is subject to the stipulations of this policy. The CA's role and the corresponding CA procedures shall be defined in a CPS. Primarily, the CA's responsibilities are to ensure that the following functions occur according to the stipulations of this policy:

- RA functions as described in Section 5.2.1.2, if no separate RA is employed;
- certificate generation and revocation;
- posting certificates and CRLs;
- performing the incremental database backups;
- administrative functions such as compromise reporting and maintaining the database;
- hardware cryptographic module programming and management, if appropriate.

5.2.1.2 Registration Authority

Any RA, which operates under this policy, is subject to the stipulations of this policy, and of the PMA approved CPS under which it operates. Primarily, an RA's responsibilities are:

- verifying identity, either through personal contact, or via Trusted Agents or employees, when allowed by this policy;
- entering Subscriber information, and verifying correctness;
- securely communicating requests to and responses from the CA;
- receiving and distributing Subscriber certificates.

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

5.2.1.3 Other Trusted Roles

For CLASS 3 and CLASS 4 assurance infrastructures, a CMA shall, in its CPS, define other trusted roles to which shall be allocated responsibilities that ensure the proper, safe, and secure operation of the CMA equipment and procedures. These responsibilities include:

- initial configuration of the system, including installation of applications, initial setup of new accounts, configuration of initial host and network interface;
- performance of compliance audit;
- creation of devices to support recovery from catastrophic system loss;
- performance of system backups, software upgrades and recovery;
- perform secure storage and distribution of the backups and upgrades to an off-site location;
- change of the host or network interface configuration;
- assignment of security privileges and access controls of Subscribers;
- performance of archive and deletion functions of the security audit log and other archive data as described in Sections 4.5 and 4.6 of this document;
- review of the security audit log.

To ensure system integrity, the CMAs shall be prohibited from performing these responsibilities for their own CMA facility. The CMA shall maintain lists, including names, organizations, and contact information, of those who act in these trusted roles, and shall make them available during compliance audits.

5.2.1.4 PKI Sponsor

A PKI Sponsor fills the role of a Subscriber for non-human system components and organizations that are named as public key certificate subjects. The PKI Sponsor works with the CMAs and (when appropriate) their Trusted Agents to register components (routers, firewalls, etc.) in accordance with Section 3.1.10, and is responsible for meeting the obligations of Subscribers as defined throughout this document.

5.2.1.5 Online Certificate Status Protocol (OCSP) Responder

Any OCSP Responder, which operates under this policy, is subject to the stipulations of this policy, and of the PMA approved CPS under which it operates. Primarily, an OCSP Responder is responsible for:

- Providing certificate revocation status and/or complete certification path validation (including revocation checking) to the relying parties; and

- Ensuring that the status and validation responses contain authentication and integrity services commensurate with the assurance level of the certificate being checked.

5.2.2 Separation of Roles

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

5.3 PERSONNEL CONTROLS

5.3.1 Background, 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. CMAs may be US uniformed service members, or government civilian employees (Federal, State, or local) of any organization authorized by the PMA to possess and issue DoD PKI certificates in accordance with Section 1.3.3.1 of this CP, or such organizations' contractors. All CMAs shall be US citizens. All persons filling trusted roles other than CMAs shall be US citizens or hold a US security clearance.

All CA operations, and Centralized OCSP Responders shall be administered by a person or body (e.g., a Board of Directors). This person or body shall be identified as the CA or OCSP Responder as described in Sections 1.3.1 and 5.2.1.1. For CLASS 4 assurance, CAs and Centralized OCSP Responders shall be administered by a military commissioned or warrant officer, government employee GS-7 or above, or a civilian contractor/vendor employee of equivalent or greater responsibility and compensation. The operators and equipment for a CA and Centralized OCSP Responder installation must be within the administrative control of the identified administrator.

Personnel appointed to operate CMA equipment within the DoD PKI may be military, civilian, or contractor personnel and 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 knowingly been previously relieved of CMA or Communications Security (COMSEC) custodian duties for reasons of negligence or non-performance of duties;
- have not knowingly 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.

CMAs issuing or requesting certificates asserting security clearances (e.g., CONFIDENTIAL, SECRET, TOP SECRET) shall hold a security clearance equal to or higher than the clearance being asserted. CMAs need not themselves hold other authorizations asserted in the certificates (e.g., security categories), unless the policy associated with these authorizations so requires.

5.3.2 Background check procedures

Local service, agency, or community procedures shall be followed to determine the need for and extent of background checks. Such checks are to be performed solely to determine the suitability of a person to fill a PKI role, and shall not be released except as required in Section 2.6. Background check procedures shall be described in the CPS.

5.3.3 Training requirements

All personnel involved in the CMA operation shall be appropriately trained. Topics shall include the operation of the CMA software and hardware, operational and security procedures, and the stipulations of this policy and local guidance. The specific training required will depend on the equipment used and the personnel selected. A training plan shall be established for a CMA installation, and training completed by the personnel shall be documented.

5.3.4 Retraining frequency and requirements

Those involved in filling PKI roles shall be aware of changes in the CMA operation. Any significant change to the CMA 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, and relocation of CA equipment.

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 PKI service.

5.3.6 Sanctions for unauthorized actions

A CMA shall take appropriate administrative and disciplinary actions against personnel who violate this policy.

5.3.7 Contracting personnel requirements

Contractor personnel employed to operate any part of the PKI shall be subject to the same criteria as a US Government employee, and cleared to the level of the information protected by the certificates the PKI issues.

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

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.

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key pair generation

This policy does not preclude any source of key, which has been generated in accordance with the stipulations of this policy and local security requirements. A private key is considered to be generated by the PKI entity that first comes into possession of it: a Subscriber, an RA, or a CA.

Cryptographic keying material for certificates issued by the CA shall be generated in FIPS 140 validated cryptographic modules. CA and OCSP Responder Cryptographic keying material and Class 4 Subscriber keys shall be generated in FIPS 140 Level 2 validated cryptographic modules. A private key must not appear outside of the module in which it was generated unless it is encrypted for local transmission or for processing or storage by a key recovery mechanism.

6.1.2 Private key delivery to Subscriber

See paragraph 4.2.1.

6.1.3 Key sizes

Digital Signature Standard (DSS) keys issued by a US DoD PKI shall use at least 160-bit private key (x) and at least 1024 bit prime modulus (p). Minimum Subscriber public key sizes shall be 1024 bits for Key Exchange Algorithm (KEA) and Rivest, Shamir, Adleman (RSA). For CLASS 2 and CLASS 3, Elliptic Curve Digital Signature Algorithm key prime field (*//p//*) shall be not less than 224, and the Binary Field (*m*) shall be not less than 233. For CLASS 4, Elliptic Curve Digital Signature Algorithm key prime field (*//p//*) shall be not less than 384, and the Binary Field (*m*) shall be not less than 409.

Use of SSL or another protocol for communication of registration information or private key delivery shall require, at a minimum, use of a symmetric key length and algorithm of workfactor equal to or greater than the workfactor associated with the subscriber key pairs.

6.1.4 Public key parameters generation

Public key parameters shall always be generated and checked in accordance with the standard that defines the cryptoalgorithm in which the parameters are to be used. For example, public key parameters for use with algorithms defined in the *Digital Signature Standard* [FIPS 186-2] shall be generated and tested in accordance with [FIPS 186-2]. Public key parameters for use with the RSA algorithm defined in [PKCS-1] shall be generated and checked in accordance with [PKCS-1], and so on. Whenever a cryptoalgorithm is described in [FIPS 186-2], the parameter generation and checking requirements and recommendations of [FIPS 186-2] shall be required of all entities generating key pairs whose public components are to be certified by the DoD PKI.

6.1.5 Parameter quality checking

See Section 6.1.4.

6.1.6 Hardware/software key generation

All keys, and intermediate keys and pseudo-random numbers used for all key generation shall be generated using a FIPS approved method.

CLASS 3 HARDWARE and CLASS 4 assurance signature key pairs shall be generated on the subscriber token.

CLASS 3 hardware assurance encryption key pairs may be generated off the token as long as there are assurances that no copies other than authorized key escrow copies of the keys continue to exist after the generation and insertion processes have completed.

CLASS 4 assurance encryption key pair shall be generated on a hardware 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 continues to exist after the generation and transfer processes have completed.

Random numbers for **CLASS 4** key material are to be generated by a hardware module.

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

Public keys that are bound into certificates which assert the CLASS 2, CLASS 3 or CLASS 4 assurance policies shall be certified for use in signing or encrypting, but not both. The use of a specific key is determined by the key usage extension in the X.509 certificate. This restriction is not intended to prohibit use of protocols (like the Secure Sockets Layer) that provide authenticated connections using encryption certificates.

6.2 PRIVATE KEY PROTECTION

6.2.1 Standards for cryptographic module

The relevant standard for cryptographic modules is *Security Requirements for Cryptographic Modules* [current version of FIPS140]. The PMA may determine that other comparable validation, certification, or verification standards are sufficient. These standards will be published by the PMA. Cryptographic modules shall be validated to the FIPS 140 level identified in this section, or validated, certified, or verified via one of the standards published by the PMA.

Subscribers who have keys certified under **CLASS 2** or **CLASS 3** shall use cryptographic modules, which meet at least the criteria specified for Level 1. **CLASS 4** certificates require Level 2 hardware cryptographic modules. A higher level may be used if available or desired. A PKI should provide the option of using any acceptable cryptographic module, to facilitate the management of Subscriber certificates.

CLASS 2 CAs may use hardware or software cryptographic modules for CA key generation and protection, validated at Level 2. **CLASS 3** certificates shall be signed using a hardware cryptographic module that meets Level 2. **CLASS 4** certificates shall be signed using a hardware cryptographic module that meets Level 2.

CLASS 2, CLASS 3, and CLASS 4 OCSP Responders that are expected to service less than 100,000 Relying Parties may use hardware or software cryptographic modules for OCSP Responder key generation and protection, validated at Level 2 or higher. All other OCSP Responders shall use Level 2 or higher hardware cryptographic modules.

CLASS 2 RAs may use hardware or software cryptographic modules that meet the criteria specified for Level 1. **CLASS 3** and **CLASS 4** RAs use hardware cryptographic modules at Level 2.

All cryptographic modules shall be operated such that the private asymmetric cryptographic keys shall never be output in plaintext. No private key shall appear unencrypted outside the CA equipment.

No one shall have access to a private signing key but the Subscriber. Private decryption keys shall only be held by parties authorized by the DoD KRP. These keys shall be held in the strictest confidence and controlled as described in the DoD Key Recovery Policy (KRP).

Private keys used to sign certificates that will assert security privileges are classified at the same level as the classification asserted in the certificate. In the case where the CA will not independently verify security privilege information, this requirement extends to RA private keys.

Note that Section 6.1.1 stipulates cryptographic module requirements for key generation.

CLASS 2	Subscriber	RA	CA	OCSP Responder

	Level 1	Level 1 (hardware or software)	Level 2 (hardware or software)	Level 2
Operational requirement	Shall not output private asymmetric key in plaintext			

CLASS 3	Subscriber	RA and CA	OCSP Responder
FIPS 140-1 validation	Level 1	Level 2 (hardware)	Level 2**
Operational requirement	Shall not output private asymmetric key in plaintext		

CLASS 3 HARDWARE	Subscriber	RA and CA	OCSP Responder
FIPS 140-1 validation	Level 1 (software for generation; insertion onto Level 1 hardware) *	Level 2 (hardware)	Level 2**
Operational requirement	Shall not output private asymmetric key in plaintext		

* = Level 1 hardware overall with Level 2 roles and services and Level 2 physical security.

CLASS 4	Subscriber	RA and CA	OCSP Responder
Current version of FIPS 140 validation	Level 2 (hardware)	Level 2 (hardware)	Level 2**
Operational requirement	Shall not output private asymmetric key in plaintext		

** = Level 2 Hardware required for Centralized OCSP Responders.

6.2.2 Private key multi-person control

For CAs and Centralized OCSP Responders expected to service 100,000 or more Subscribers, a single person shall not be permitted to invoke the complete CA or OCSP signature or access any cryptographic module containing the complete CA or OCSP Responder private key. Access to CA or OCSP Responder signing keys backed up for disaster recovery shall be under at least two-person control.

CLASS 3 and CLASS 4 private key management keys requested by other than the subscriber/PKI sponsor, may only be extracted from key recovery databases under two-person control. CMAs may back up key management and signature keys in multiple cryptographic modules without two-person control so long as the CMA backup actions are recorded for security audit. For CLASS 2 and CLASS 3, Subscribers are permitted to back-up their own encryption (but not signature) private keys. Only CAs may back up CLASS 4 encryption (but not signature except for the NSM CAW) private keys in multiple cryptographic modules on behalf of Subscribers; neither RAs nor Subscribers shall back up CLASS 4 private keys. CA and OCSP Responder signature keys may only be backed up 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.

6.2.3 Private key escrow

Under no circumstances shall a key used to support non-repudiation services be held in trust by a third party.

For some purposes (such as data recovery) it shall be necessary to provide key retrieval for the private component of the encryption certificate key pair. To facilitate this the PKI shall provide a key escrow capability. The method, procedures and controls which will apply to the storage, request for, extraction and/or retrieval, delivery, protection and destruction of the requested copy of an escrowed key shall be described in a Key Recovery Policy (KRP) which shall become an integral component of this CP.

6.2.4 Private key backup

For CLASS 2 and CLASS 3, Subscribers are permitted to back-up 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 requires the key in a different location or format. CLASS 2 and CLASS 3, except for CLASS 3 Hardware, Component PKI Sponsors (see Section 3.1.10)

are authorized to make a single backup copy of the component private keys to support backup in cases where component malfunction results in key corruption. All key transfers shall be done from an approved cryptographic module, and the key shall be encrypted during the transfer. The Subscriber (PKI Sponsor for Components) is responsible for ensuring that all copies of private keys, including those that might be embedded in component backups, are protected including protecting any workstation on which any of its private keys reside.

A CA may only copy a Subscriber's hardware cryptographic module in response to a valid initial request for a backup, or as a result of an administrative action form request signed by the Subscriber. Every access authorization shall be documented, and each resultant access recorded. Only CAs and Subscribers shall back-up private keys (RAs shall not back-up private keys).

CA private signature keys may be backed up under the same multi-person control as the original signature key. No more than two backup copies of the CA private signature keys may be made. If backups are made, only a single copy of any signature key is to be kept at the CA location; if a second copy is made, it shall be kept at a backup location.

OCSP Responder's private signature keys shall be backed up as defined in section 6.2.2. No more than two backup copies of the OCSP Responder's private signature keys may be made. The backup module shall also meet the cryptographic module requirements for the OCSP Responder. If backups are made, only a single copy of any signature key is to be kept at the OCSP Responder location; if a second copy is made, it shall be kept at a backup location.

The Class 4 FORTEZZA CAW sites may require backup CA material to comply with Disaster Recovery Plans and other instances requiring additional backup CA material. The DoD PCA is authorized to create up to two copies of a CA key for a primary site and an additional copy for each of up to two approved backup sites, upon receipt of a valid request from the CAW site and approval by the Service or Agency CAW Approval Authority. The backup site locations need not be disclosed in the request. In addition, upon receipt of a valid request from the CAW site and approval by the Service or Agency CAW Approval Authority attesting to the non-functional status and destruction of one of the original copies created, the PCA is authorized to create an additional replacement copy. Valid requests for CAW CA Materials in excess of the above-stated quantities shall additionally require PCA approval.

6.2.5 Private key archival

See Section 6.2.3 and Section 6.2.4.

6.2.6 Private key entry into cryptographic module

Private keys are to be generated by and in a cryptographic module. In the event that a private key is to be transported from one cryptographic module to another, the private key must be encrypted during transport; private keys must never exist in plaintext form outside the cryptographic module boundary.

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

6.2.7 Method of activating private key

Pass-phrases, Personal Identification Number (PINs), biometric data, or other mechanisms of equivalent authentication robustness must be used to activate the private key in a cryptographic module. [Activation data generation requirements are specified in 6.4.1] Activation data may be distributed in person, or mailed to the Subscribers separately from the cryptographic modules that they activate. Entry of activation data must be protected from disclosure (e.g., the data should not be displayed while it is entered).

6.2.8 Method of deactivating private key

Cryptographic modules, which have been activated, must not be left unattended or otherwise open to unauthorized access. After use, they must be deactivated, e.g. via a manual logout procedure, or by a passive timeout. Hardware cryptographic modules shall be removed and stored when not in use.

6.2.9 Method of destroying private key

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

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public key archival

The public key is archived as part of the certificate archival.

6.3.2 Usage periods for the public and private keys

The key usage periods for keying material is described in Section 3.2.

If the CA key cryptoperiod is shorter than the end-entity cryptoperiod, then the RA key cryptoperiod shall be no longer than the CA key cryptoperiod.

6.4 ACTIVATION DATA

6.4.1 Activation data generation and installation

Activation data may be Subscriber selected. A pass-phrase, PIN, biometric data, or other mechanisms of equivalent authentication robustness shall be used to protect access to use of a private key. Activation data shall meet the "strength of authentication mechanism" requirements in section 4.3.3 [FIPS 140-2].

Subscriber (to include CMAs) PINs, when used, shall be 6-8 digits at a minimum. Randomly generated PINs shall be used when possible. If 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; are not repeated numbers or sequences, nor are easily guessed numbers. When alphanumeric pass-phrases are used, a mix of 8 characters, including at least two interspersed digits, shall be used. The activation data 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 activation data shall not contain sequences, repeated characters, date formats, or license plate formats. To the extent practicable (Note: may not be possible if the PIN is entered directly at the card reader), technical means shall be used to verify that the activation data meets all of the requirements in this section.

If random numbers are used to generate PINs or pass-phrases, they shall meet all the applicable [FIPS 140-2] requirements. The method used to derive PIN or pass-phrase characters from the random numbers shall ensure that all valid characters for the PIN or pass-phrase are selected with equal probability (e.g., generate a random number (with 8 bits of entropy) and either use it if it corresponds to the American Standard Code for Information Interchange (ASCII) representation of an element of the valid character set, or otherwise reject it and obtain an additional 8 bits of random data and repeat).

If the activation data must be transmitted, it shall be via a channel of appropriate protection, and distinct in time and place from the associated cryptographic module. If this is not done by hand, the Subscriber shall be advised of the shipping date, method of shipping, and expected delivery date of any activation data. As part of the delivery method, Subscribers will sign and return a delivery receipt. In addition, Subscribers should also receive (and acknowledge) a Subscriber advisory statement to help to understand responsibilities for use and control of the cryptographic module.

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.

Activation data for private keys associated with certificates asserting individual identities shall never be shared. Activation data for private keys associated with certificates asserting organizational identities shall be restricted to those in the organization authorized to use the private keys.

6.4.3 Other aspects of activation data

CLASS 3 and CLASS 4 CMAs shall change their CMA cryptographic module activation data whenever the CMA token is returned for maintenance or rekey.

6.5 COMPUTER SECURITY CONTROLS

CA and OCSP Responder equipment used for CLASS 3 assurance infrastructures shall use operating systems that:

- Require authenticated logins
- Provide discretionary access control
- Provide a security audit capability

CA and OCSP Responder equipment used for CLASS 4 assurance infrastructures shall be hosted on operating systems that implement the requirements of CLASS 3, plus:

- Trusted path
- CA application that was developed using Trusted System Development Methodology (TSDM) Level 2,was evaluated for compliance with Certificate Issuing & Management Component (CIMC) Protection Profile, Level 3, or a comparable PMA approved standard.
- OCSP Responder shall be evaluated for compliance with Common Criteria (CC) Evaluation Assurance Level (EAL) 4 or a comparable PMA approved standard.

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

6.6 LIFE CYCLE TECHNICAL CONTROLS

Equipment (hardware and software) procured to operate a PKI shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with, such as random selection. Equipment developed for a PKI shall be developed in a controlled environment. For **CLASS 4**, the development process shall be defined and documented.

All hardware and software that has been identified as supporting a Centralized OCSP Responder or a CLASS 3 or CLASS 4 CA, must be shipped or 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 and OCSP Responder (for those OCSP Responders specified above in this paragraph) 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.

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

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

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

For classified applications, the CA equipment and cards will be shipped via the COMSEC Material Control System (CMCS) if any classified application software has been loaded, or if any classified information has ever been loaded on the equipment or cards.

CLASS 2, CLASS 3	Purchase in manner to reduce likelihood of tampering, or develop in controlled environment Protective packaging, accountable delivery method
CLASS 4	Developed via documented controlled process Tamper-evident packaging, controlled delivery method for CA equipment and end-entity cryptographic module

6.7 NETWORK SECURITY CONTROLS

CMA equipment shall be located on internal networks behind boundary/perimeter network defenses and afforded protections consistent with GIG IA Policy for network security at the Mission Assurance Category I (MAC I) level. Services allowed to and from the Class 3 and Class 4 CA 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 be stand-alone (off-line) configurations.

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 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

Requirements for cryptographic modules are as stated above in section 6.2.

7 CERTIFICATE AND CRL PROFILES

7.1 CERTIFICATE PROFILE

7.1.1 Version numbers

This policy governs only DoD X.509 Version 3 certificates. CMAs who issue or manage X.509 Version 1 certificates are subject to the *Information Systems Security Policy and Procedures for FORTEZZA Card Certification Authority Workstations* [NAG-69].

7.1.2 Certificate extensions

Rules for the inclusion, assignment of value, and processing of extensions are defined in profiles. These profiles are written to prescribe an appropriate amount of control over an infrastructure, yet be flexible enough to meet the needs of the various CAs and communities. **CLASS 4** assurance infrastructure shall use the extensions and path processing defined in *X.509 Certificate and Certificate Revocation List Profiles and Certification Path Processing Rules for MISSI* [SDN.706]. **CLASS 3** and **CLASS 2** infrastructures shall use *Federal PKI Version 1 Technical Specifications: Part E – X.509 Certificate and CRL Extensions Profile* [FPKI-Prof]. Any variance to these profiles shall be approved by the DoD PKI Technical Working Group, and documented in a CPS. Whenever private extensions are used, they shall be identified in a CPS. Critical private extensions shall be interoperable in their intended community of use.

Access control information may be carried in the subjectDirectoryAttributes extension. If this is desired, the syntax is defined in detail in [SDN702].

7.1.3 Algorithm object identifiers

Certificates under this Policy will use the following OIDs for signatures:

id-dsa-with-sha1	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3}
sha1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12}
sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13}
ecdsa-with-SHA1	{iso(1) member-body(2) us(840) ansi-x9-62 (10045) signatures (4) 1 }

Certificates under this Policy will use the following OIDs for identifying the algorithm for which the subject key was generated:

id-dsa	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1}
Id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-x9-62(10045) public-key-type (2) 1}
rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}
id-keyExchangeAlgorithm	{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22}

The DoD PKI shall certify only public keys associated with the cryptoalgorithms identified above, and shall only use the signature cryptoalgorithms described above to sign certificates, certificate revocation lists and any other PKI product.

7.1.4 Name forms

In general, the DN will be used throughout the DoD X.500 Directories use the DN for lookups. All PKIs shall have the ability to generate and process DNs. Some communities or installations may choose to use other names, for example certificates used to implement a hardware protocol, where device addresses are most useful and certificate lookup is not performed. In this case, an alternate name form may be included in the subjectAltName extension. If there is no DN (all CLASS 4 certificates shall have a DN), then the subject field of

the base certificate shall be an empty sequence, and that extension shall be marked critical. Any name form defining GeneralName in [ISO9594-8] may be used, in accordance with the required profile (Section 7.1.2).

Use of alternate name forms shall be defined in a CPS, including criticality, types, and name constraints.

7.1.5 Name constraints

CA certificates issued under a **CLASS 4** PKI shall impose name constraints and path length constraints as required by [SDN.706].

7.1.6 Certificate policy object identifier

Certificates issued under this policy shall assert the OID appropriate to the level of assurance with which it was issued, as defined in Section 1.2.

7.1.7 Usage of policy constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

Certificates issued under this policy shall not contain policy qualifiers.

7.1.9 Processing semantics for the critical certificate policy extension

This policy does not require the certificatePolicies extension to be critical. Relying Parties whose client software does not process this extension, risk using certificates inappropriately.

7.2 CRL PROFILE

7.2.1 Version numbers

CRLs issued under this Policy shall assert a version number as described in the X.509 standard [ISO9594-8]. Class 4 CRLs shall assert Version 2. **CLASS 2** and **CLASS 3** CRLs may assert Version 1 or Version 2.

7.2.2 CRL and CRL entry extensions

Detailed CRL profiles covering the use of each extension are available in [SDN706]. Certificates issued by a **CLASS 2** or **CLASS 3** PKI may alternately conform to the profile recommendations in [FPKI-Prof], or may issue CRLs asserting no extensions. Any variance to these profiles shall be approved by the DoD PKI Technical Working Group, and documented in a CPS.

8 CERTIFICATE POLICY ADMINISTRATION

8.1 SPECIFICATION CHANGE PROCEDURES

The PMA shall review this policy at least once every year. The PMA shall maintain and publish a Certificate Policy Plan that describes anticipated changes to this CP. Errors, updates, or suggested changes to this document shall be communicated to the contact in Section 1.4. Such communication must include a description of the change, a change justification, and contact information for the person requesting the change.

All policy changes under consideration by the PMA shall be disseminated to interested parties (see Section 8.2) for a period of at least one month.

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

8.2 PUBLICATION AND NOTIFICATION POLICIES

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

The PMA will maintain a list of CAs asserting this policy (this responsibility may be delegated to a Root- or Intermediate-CA in practice). Proposed changes to the policy and 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.

8.3 CPS and External Policy Approval Procedures

The PMA shall make the determination that a CPS complies with this policy for a given level of assurance. The CMA must have and meet all requirements of an approved CPS prior to commencing operations. In some cases the nature of the system function, the type of communications, or the operating environment may require the additional approval of an authorized agency.

The Policy Management Authority is authorized to make the determination that other (non-DoD) CPs offer appropriately equivalent levels of assurance to the DoD CPs. The PKI 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 CPs, in DoD OCSP Responders, or;
- recommending CAs asserting other CPs for inclusion in DoD application trust lists.

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

8.4 WAIVERS

Normally, the PMA shall decide that variation in CMA practice is acceptable under a current policy, or the CMA shall request a permanent change to the policy. Policy waivers may be granted by the PMA to meet urgent, unforeseen operational requirements (such as those associated with ongoing military actions or a similar crisis). When a waiver is granted, the PMA shall post the waiver on a web site accessible by relying parties, and shall either initiate a permanent change to the policy, or shall place a specific time limit, not to exceed one year, on the waiver.

BIBLIOGRAPHY

The following documents contain information which provide background, examples, or details about the contents of this policy:

ABADSG	*Digital Signature Guidelines,* 1996-08-01. http://www.abanet.org/scitech/ec/isc/dsgfree.html.
FOIACT	5 U.S.C. 552, Freedom of Information Act. http://www4.law.cornell.edu/uscode/5/552.html
ITMRA	40 U.S.C. 1452, Information Technology Management Reform Act of 1996. http://www4.law.cornell.edu/uscode/40/1452.html
PKCS#12	*Personal Information Exchange Syntax Standard*, April 1997. http://www.rsa.com/rsalabs/pubs/PKCS/html/pkcs-12.html
NAG69C	*Information System Security Policy and Certification Practice Statement for Certification Authorities, rev C,* November 1999.
NSD42	*National Policy for the Security of National Security Telecom and Information Systems*, 5 Jul 90. http://snyside.sunnyside.com/cpsr/privacy/computer_security/nsd_42.txt (redacted version)

ACRONYMS AND ABBREVIATIONS

ASCII	American Standard Code for Information Interchange
CA	Certification Authority
CMA	Certificate Management Authority
CMCS	COMSEC Material Control System
COMSEC	Communications Security
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DAA	Designated Approving Authority
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DN	Distinguished Name
DoD	Department of Defense
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
FIPS	Federal Information Processing Standard
FPKI	(US) Federal Public Key Infrastructure
GS-	General Schedule (Federal civilian level)
HAG	High Assurance Guard
ICRL	Indirect Certificate Revocation List
ID	Identity (also, a credential asserting an identity)
INE	In-Line Encryptors
ISSO	Information System Security Officer
ITSEC	Information Technology Security Evaluation and Certification
KEA	Key Exchange Algorithm
KMI	Key Management Infrastructure
KRP	Key Recovery Policy
MD	Maryland
NIPRNET	Non-classified Internet Protocol Router Network
NSA	National Security Agency
NSD	National Security Decision
NSM	Network Security Managers
NSSI	National Security System Information
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OCSP	Online Certificate Status Protocol Responder

Responder	
OID	Object Identifier
PAA	Policy Approving Authority
PCA	Policy Creation Authority
PIN	Personal Identification Number
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PMA	Policy Management Authority
RA	Registration Authority
RD	Road
RSA	Rivest, Shamir, Adleman (encryption algorithm)
SIPRNET	Secret Internet Protocol Router Network
TSDM	Trusted System Development Methodology
US	United States

GLOSSARY

The primary source is *NSTISSI 4009, National Information Systems Security Glossary*; other sources were used if NSTISSI 4009 had no entry for the term, or if another source gave 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. [NS4009]
access control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009]
accreditation	Formal declaration by a Designated Approving Authority that an IS is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]
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]
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, and to recommend necessary changes in controls, policies, or procedures. [NS4009]
audit data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]
authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009]
backup	Copy of files and programs made to facilitate recovery if necessary. [NS4009]
binding	Process of associating two related elements of information. [NS4009]
biometric	A physical or behavioral characteristic of a person.

Certificate Management Authority (CMA)	A Certification Authority, a Registration Authority or an OCSP Responder issued a DoD PKI certificate.
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. [ISO9594-8]
CA facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
Centralized OCSP Responder	An OCSP Responder that provides OCSP responses to over 100,000 Relying Parties.
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-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.
client (application)	A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.
compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]
confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
cryptographic module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS1401]
cryptoperiod	Time span during which each key setting remains in effect. [NS4009]
DITSCAP	DITSCAP establishes a standard DoD-wide process, set of activities, general tasks, and a management structure to certify and accredit Information Systems (IS) that will maintain the Information Assurance (IA) and security posture of the DII throughout the life cycle of the system.
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.
firewall	Gateway that limits access between networks in accordance with local security policy. [NS4009]
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.
Information System Security Officer (ISSO)	Person responsible to the designated approving authority for ensuring the security of an information system throughout its lifecycle, from design through disposal. [NS4009]
inside 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	Protection against unauthorized modification or destruction of information. [NS4009]
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.
Mission Assurance Category.	Mission Assurance Category. Applicable to DoD information systems, the mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. The Department of Defense has three defined mission assurance categories: Mission Assurance Category I (MAC 1). Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or

availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. Mission Assurance Category I systems require the most stringent protection measures.

Mission Assurance Category II (MAC II). Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. Mission Assurance Category II systems require additional safeguards beyond best practices to ensure adequate assurance.

Mission Assurance Category III (MAC III). Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. Mission Assurance Category III systems require protective measures, techniques or procedures generally commensurate with commercial best practices.

Note: Corresponding references within the CP to old Mission category terms Mission Critical (including subcategories), Mission Support and Administrative should also be changed to MACI, MACII, and MACIII, respectively. (A quick scan of CP indicates the following number of instances of each term: Mission critical including subcategories (7); Mission support (3); Administrative (3).

naming authority	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
National Security System	Any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [ITMRA]
NIPRnet	Unclassified router-based data network system, part of the Defense Information Infrastructure.
non-repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009]
OCSP Responder	A trusted entity that provides on-line revocation status of certificates to Relying Parties.
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 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.
rekey (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application.
Relying Party	A person who has received a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them. [ABADSG]
renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
repository	A trustworthy system for storing and retrieving certificates or other information relevant to certificates. [ABADSG]
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	Classified router-based, data network system, 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. [NS4009]
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 cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]
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 providing Subscriber identification 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	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed, and each familiar with established security and safety requirements. [NS4009]
update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS1401]

9 CP V8.0 Change Proposal Summary Table

Change Serial Number: CPM 2003 – 01

Title: Activation Data Generation and Installation

Change Advocate Contact Information:
Name: Deborah S. Gallagher
Organization: Defense Manpower Data Center, DoD Access Card Office
Telephone number: 703- 696 - 7418
E-mail address: Gallagds@osd.pentagon.mil

Applicable Section: 6.4.1

Change Summary:
Changes paragraph 6.4.1 to delete the requirement for Class 4 pass-phrase or PIN to be randomly and automatically generated.

Background:
The DoD Class 2 and Class 3 level PIN or pass-phrase to protect the private key can be subscriber selected. Any pass-phrase or PIN will be generated in conformance with FIPS 112. As currently stated in the X.509, any Class 4 pass-phrase or PIN must be randomly and automatically generated. This change would allow the user to more easily remember his/her pass-phrase or PIN and also avoid the cost associated with returning to have pass-phrases or PINs reset. FIPS112 section 3.1 states "The set of acceptable passwords must be such that it can be specified easily, that acceptable passwords can be generated or selected easily, that a valid password can be remembered, can be stored reasonably and can be entered easily."

Change Serial number: CPM 2003 – 10

Title: Certificate Status Authority (CSA) Security

Change advocate contact information:
Name: Sharron Kegler
Organization: DISA/API2
Telephone number: 703-882-1638
Email address: KeglerS@ncr.disa.mil

Applicable Sections: 1,3,1, 2.1.6, 4.4.4, 4.5.1, 5.1.2, 5.2.1, 5.2.1.5, 6.2.1, 6.2.4, 6.5, 6.6, 6.7

Change Summary:
The CP needs to define obligations and security of Certificate Status Authority (CSA). Examples of CSA include, but are not limited to, SCVP Responder and OCSP Responder.

Change Serial Number: CPM 2003 - 13

Title: Additional algorithm identifiers for new RSA signature algorithms

Change Advocate Contact Information:
Name: Dave Fillingham
Organization: NSA/V51
Telephone number: 410-854-4537

E-mail address: dwfilli@missi.ncsc.mil

Applicable Section: 7.1.3

Change Summary:
Change the algorithm object identifier list to add the new RSA signature algorithm identifiers that are based on the emerging SHA-256, SHA-384, and SHA-512 hash algorithms. Change the existing RSA algorithm object identifier to correct a typographical error.

Background:
The current DoD PKI implementation is based on the use of the SHA-1 hash algorithm in accordance with the existing FIPS 180-1, Secure Hash Standard. Currently, the SHA-1 algorithm is used in conjunction with the RSA encryption algorithm with a 1024-bit RSA modulus. The SHA-1 hash algorithm has a commensurate strength for use with 1024-bit RSA. However, it is not commensurate with larger RSA modulus sizes.

The DoD Key Management Infrastructure (KMI) Program anticipates the use of a larger RSA modulus in either the current Capability Increment (CI-1) or in future increments (CI-2). In accordance with good key management practices, it is desirable to use a hash algorithm with a strength that is greater than or equal to the strength of the RSA modulus.

FIPS 180-1 is currently under revision. A mature draft of its replacement (FIPS180-2) is available from the National Institute of Standards and Technology (NIST). The sole purpose for the revision is to add "three algorithms that are capable of producing larger message digests", namely SHA-256, SHA-384, and SHA-512. FIPS 180-2 is expected to receive final approval shortly.

RSA Security Inc. has recently released an updated version of the RSA Cryptography Standard (PKCS #1 v2.1, 14 June 2002). In anticipation of NIST approval, RSA has already registered new RSA signature algorithms that incorporate the use of the new SHA algorithms in conjunction with the RSA encryption algorithm. In fact, PKCS #1 v2.1 clearly states that "SHA-1 and SHA-256/384/512 are recommended for new applications." It also specifies the new PKCS #1 object identifiers (OIDs) for these new signature algorithms. This change proposal adds the new OIDs to the existing list of algorithm object identifiers specified in section 7.1.3 of the CP.

This change proposal also provides a minor correction to the existing OID for SHA-1. According to PKCS #1, the OID for SHA-1 used with RSA encryption is "sha1WithRSAEncryption" not "sha-1WithRSAEncryption".

This change proposal makes no change to the DSA or ECDSA object identifiers.

They are included below only for the purpose of completeness.

Change Serial number: **CPM 2003 - 15**

Title: Power and air conditioning (Environmental Controls)

Change advocate contact information:
Name: Carl C. Wardell
Organization: NSA/V51
Telephone number: (410) 854-4537
Email address: ccwarde@missi.ncsc.mil

Applicable Section: 5.1.3

Change Summary:
The intent of the language in section 5.1.3 is to ensure that in the event of a power outgage the CA's will not shut down before important procedures can be performed. To ensure this an uninterruptible power supply or a power generator would prevent undesired features of the power source (outages, sags, surges, bad harmonics, etc.) from adversely affecting the performance of the CA. However, the language in the current CP is unclear. It could be interpreted to imply that the back-up source of power for the CA would have capabilities to automatically lockout input, finish pending actions and record the state of the equipment before lack of power or air conditioning causes a shutdown could be interpreted that CA equipment must automatically perform these functions and the internal KMI power supply must have sufficient back-up power to allow this. Neither interpretation is technically feasible with existing COTs products.

Background:
The intent of the language in section 5.1.3 is to ensure that the CA's will not immediately shutdown due to a power failure (possibly resulting in the corruption of CA data/status) but will instead have sufficient backup power to ensure that operators can command the CA to shutdown normally. Release 3 currently meets the intent of the requirement. The Class 3 CA CPS states the following: "The Class 3 CA will be housed and operated in a DECC, and will therefore have available all necessary utilities support. The power supply will be UPS."

Change Serial Number: CPM 2003 - 16

Title: Personnel Controls for CMAs

Change Advocate Contact Information:
Name: Gary Strohm
Organization: DIA/SYS-4
Telephone number: (202) 231-2018/DSN (312) 428-2018
E-mail address: gary.strohm@dia.mil

Applicable Section: 5.3.1

Change Summary:
Allow organizations authorized in 1.3.3.1 to be subscribers to have their own govt civilian employees function as CMAs (RA/LRAs) vs. current limitation to being only DoD civilian, military, contractor.

Background:
5.3.1 paragraph 1 currently requires RAs to be DoD uniformed service members, DoD civilians, or contractors, requiring all CMAs and those filling trusted roles other than CMAs to be US citizens. 1.3.3.1 allows for issuance of certificates to other executive departments personnel and their contractors, state govts, foreign govts etc.
5.3.1 paragraph 3 states "personnel authorized to operate CMA equipment within the DoD may be military, civilian, or contractor personnel and shall." As written, it could be interpreted that other entities authorized by 1.3.3.1 must utilize either a DoD uniformed service member or a contractor as an RA, not a government civilian employee.

Change Serial number: CPM 2003 - 18

Title: Allow creation of copies of Class 4 FORTEZZA CA private key

Change advocate contact information:
Name: Ms. Kathy Reading
Organization: NSA/Y18
Telephone number: 410 526-3107
Email address: k.readin@radium.ncsc.mil

Applicable Section: 6.2.4

Change Summary:
Permit the DoD Policy Creation Authority (PCA) in support of the Class 4 FORTEZZA infrastructure to create backup CA material upon receipt of valid requests to support Disaster Recovery Plans and other site requirements.

Background:
This change proposal is submitted to ensure the DoD PCA is in compliance with the DoD Certificate Policy, in support of Class 4 FORTEZZA CA Requests to create backup copies of the CA keys. The applicable paragraphs of the DoD CP make the DoD PCA non-compliant by creating more than two backup copies of the CA key.

The DoD CP was changed to be consistent with the X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA CP), which requires that no more than one copy of the CA signing key be kept as backup at the CA facility.

Current DoD PCA practice requires exemption from this change to meet the needs of the Class 4 FORTEZZA infrastructure.

Change Serial Number: CPM 2003 - 20

Title: CMA Compliance Audit

Change advocate contact information:
Name: Sharron Kegler
Organization: DISA/API1
Telephone number: 703-882-1638
Email address: KeglerS@ncr.disa.mil

Applicable Sections: 2.5.5, 2.5.6

Change Summary:
The CP needs to define actions that should be taken as a result of deficiency of compliance audits.

Change Serial Number: CPM 2003 - 21

Title: Statement of PMA Decision Authority

Change Advocate Contact Information:
Name: Lawrence J. Frank
Organization: USAF/XICII
Telephone number: 703-588-6115
E-mail address: lawrence.frank@pentagon.af.mil

Applicable Section: 1.3.1

Change Summary:
Specifies the PMA decisions authority and the delegation of authority for day-to-day operations.

Background:
The CP defines the "Policy Management Authority" as a "body" - but in practice - there is a body that provides recommendations and a single individual authorized to sign on behalf of the PMA. For the CP (and KRP) that is ASD/C3I. For most day-to-day operations, that is delegated to the DoD PKI PM. This CP Change proposal would document that process within the CP.

An alternative to specifying this in the DoD CP would be to specify it in the DoD PKI Policy

Change Serial Number: CPM 2003 – 22

Title: CLASS 3 and CLASS 4 Root Backup and Audit

Change Advocate Contact Information:
Name: Carl C. Wardell
Organization: NSA/V51
Telephone number: 410.854.4891
E-mail address: ccwarde@missi.ncsc.mil

Applicable Section: 5.1.8

Change Summary:
To clarify the CP regarding backups and audit requirements for the CLASS 3 and CLASS 4 Root systems.

Background:
The Electronic Key Management System (EKMS) Central Facility Finksburg (CFF) currently hosts several CLASS 3 and the CLASS 4 Public Key Infrastructure (PKI) Roots. All of the stand-alone systems and are not connected to a network. The Roots are used for two functions: to sign a subordinate Certificate Authority (CA) certificate, and to create Certificate Revocation Lists (CRLs). Upon initial stand-up of the Root systems, they sign a few CA certificates, and then are only activated to create a CRL every 14 days.

The Root systems are in a powered off mode. Every 14 days a three-person team, which consists of an Operator, System Administrator (SA), and Information Systems Security Officer (ISSO), accesses the Root room, builds a new CRL and writes it off to floppy, backs up the system, and performs an audit on each the CLASS 3 and CLASS 4 Root systems.

Physical security, procedural controls, and access controls to the Root systems are very stringent. As stated in the CLASS 3 and CLASS 4 Certification Practice Statements (CPS) and System Security Plan (SSP) for accreditation of the systems, the Root systems are protected from unauthorized access with the following controls:

- The CFF site is guarded 24 hours a day, 7 days a week.
- Within the site, the Root systems are in a separate room that is protected by an intrusion detection system.
- The room is under Two Person Access (TPA) control with access granted to an Operators, SA, and ISSO. The room must maintain two party integrity at all times while open.

- A check is made once every 24-hours by the ISSO to ensure that the door to the room is locked and that there have been no attempts at forceful entry.
- The door to the Root Room is secured under two-person control with a dead bolt key lock and combination lock. Only the personnel who have access to the room know the combination of the lock, and two individuals on an access control list must sign out the key.
- An access control list of personnel who have access to the room is posted on the outside of the Root Room door; access control lists of personnel who have access to each Root system are posted inside the room.
- Once the door to the Root room is opened, the Root systems equipment is accessible by only the members of the Root Systems Operations Team: the Operator, SA and ISSO.
- The Root Operator, SA, and ISSO roses are separate. Personnel who hold these roles at the CFF are U.S. Citizens, hold a security clearance, and are trained on system operations and PKI policy. Each of the personnel is cognizant of the system and how it operates, and oversees what the other roles are doing in the system to eliminate well-intentioned violations from privileged access.
- Root Operations personnel are given least privilege where they are granted only the privileges needed for the performance of authorized tasks.
- Each function performed on the CLASS 3 and CLASS 4 Root systems is logged in a record book. This information is reviewed as part of the bi-weekly audit by the ISSO.
- Passwords are used to protect the Root systems and private key from unauthorized access. A password is required to access the Root account. These passwords are generated manually in accordance with NSA guidance for strong passwords, and are changed every 90 days or whenever a personnel change occurs.
- A separate password is required to access the system token.
- Tokens and keys for the CLASS 3 and CLASS 4 Root systems are stored in a TPA safe when not in use. The Operator holds one combination to the TPA safe, the other is held by the ISSO.
- In addition to the audit requirements stated in the CPS, the ISSO also uses a file integrity tool on the CLASS 3 and CLASS 4 Root systems.

The stand-alone Root systems are turned off, and only accessed twice a month for CRL creation, back-up and audit. The risk of unauthorized access is low due to the physical, procedural, and access controls in place to protect the Root systems. There is no risk from network attacks as the Root systems are stand-alone. The requirement to have all 3 roles in the Root Room when the systems are being accessed minimizes the risk of collusion and insider threat.

Change Serial Number: CPM 2003 - 23

Title: Group & Role Certificates

Change Advocate Contact Information:
Name: Paul Hamilton
Organization: USMC, MCNOSC
Telephone number: 703-784-3243
E-mail address: hamiltonp@mcnosc.usmc.mil

Applicable Section: 4.2.1

Change Summary: To reword the CP to relax the requirement to tightly track the location of shared keys as allowed by the CP.

Background:
The current CP requires that the ISSO and the CA/RA closely track which individuals are holding group and role certificates. The recommended change relaxes this requirement for the ISSO/CA/RA, and allows the group/role sponsors to take responsibility for it.

Change Serial Number: CPM 2003 - 24

Title: External Certificate Authority (ECA) Reconciliation

Change Advocate Contact Information:
Name: David Bushnell
Organization: Booz Allen Hamilton
Telephone number: 410-684-6456
E-mail address: bushnell_david@bah.com

Applicable Sections: 1.3.4, 1.3.4.2, 2.4.1, 2.6.1, 3.1.8, 4.5.1, 4.8.2, 5.2.1.4, 6.1.6, 6.1.7, 6.2.1, 6.4.2, 7.1.9, Appendix E Glossary Terms

Change Summary:
The following change proposal inputs is a combined CPM, which incorporates a number of recommended changes to the X.509 DoD V7.0 CP. These changes stem from the CPMWG's review and recommended update to the DoD ECA CP.

Background:
After the review and modification of the DoD ECA CP, the CPMWG decided changes were required to the X.509 DoD V7.0 CP. These changes would bring both CPs more in line with each other.