Committee on National Security Systems

**CNSS Instruction No. 1300**
**October 2009**

# INSTRUCTION FOR NATIONAL SECURITY SYSTEMS PUBLIC KEY INFRASTRUCTURE X.509 CERTIFICATE POLICY Under CNSS Policy No. 25

**National Manager**

# FOREWORD

1. The Committee on National Security Systems Instruction (CNSSI) No. 1300, “Instruction for National Security Systems (NSS) Public Key Infrastructure (PKI) X.509 Certificate Policy, Under CNSS Policy No. 25,” provides a secure, interoperable electronic environment that closes the gap between the classified Federal PKI, managed by the Federal PKI Policy Authority, and the highly classified Intelligence Community PKI, managed by the Office of the Director for National Intelligence (ODNI).

2. The NSS operates using a hierarchical architecture, with a Root Certificate Authority (CA) operated by the National Security Agency (NSA) on behalf of the CNSS. CNSS member agencies may either establish and operate one or more CAs subordinate to the Root CA in accordance with this Certificate Policy (CP) or obtain certificates from a Common Services Provider CA operated in accordance with this CP.

3. The NSS PKI CP states the requirements for issuing and managing certificates that Relying Parties can use in making decisions regarding what assurance they can place in a certificate issued by a NSS PKI CA.

4. CNSS Instruction No. 1300 is effective upon receipt.

5. This instruction is available from the CNSS Secretariat, or the CNSS website: www.cnss.gov.

FOR THE NATIONAL MANAGER:

//s//

RICHARD C. SCHAEFFER

## Document Version Control

| Version | Date | Revision Details |
|---|---|---|
| Final 1.0 | 24 July 2009 | Final version as approved by CNSS Committee for signature |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

THIS PAGE INTENTIONALLY LEFT BLANK

# Table of Contents

# 1 INTRODUCTION

Under the provisions of *National Security Directive (NSD) 42, National Policy for the Security of National Security Telecommunications and Information Systems* [NSD 42], the Committee on National Security Systems (CNSS) has established a Public Key Infrastructure (PKI) for SECRET-high collateral classified networks, known as the National Security System (NSS) PKI. The purpose of the NSS PKI is to provide a secure, interoperable electronic environment that closes the gap between the unclassified Federal PKI, managed by the Federal PKI Policy Authority, and the highly classified Intelligence Community PKI, managed by the Office of the Director for National Intelligence (ODNI).

*CNSS Policy (CNSSP) Number 25, National Policy for Public Key Infrastructure in National Security Systems* [CNSSP 25], establishes the requirements for Federal Departments and Agencies to implement the NSS PKI to manage and support their SECRET and below collateral classified NSS networked systems.

The NSS PKI will provide the following services:

- Key generation and storage
- Certificate generation, modification, re-key, and distribution
- Key escrow and recovery of private keys associated with encryption (e.g. key management, key establishment) certificates
- Certificate Revocation List (CRL) generation and distribution
- Directory management for certificate related items
- Certificate token initialization, programming, and management
- System management functions (e.g., security audit, configuration management, archive)

The NSS PKI will operate using a hierarchical architecture, with a Root Certificate Authority (CA) operated by the National Security Agency (NSA) on behalf of the CNSS. CNSS member agencies may either establish and operate one or more CAs subordinate to the Root CA in accordance with this Certificate Policy (CP) or obtain certificates from a Common Services Provider CA operated in accordance with this CP. The NSS PKI will support the issuance of cross certificates to CNSS member agencies that are operating legacy NSS PKIs on their classified networks until such time as they fully transition to the NSS PKI. Cross certificates may also be issued to PKIs operated by non-CNSS members to support interoperability.

The NSS PKI supports the issuance of the following six types of certificates:

- Identity
- Encryption
- Signature
- Code Signing
- Content Signing
- System or Device

The distinctions between the types of certificates are primarily in the intended use of the certificates and in the information found in the *Key Usage* extension in the certificate. See Section 6.1.7 for key usage information. Complete profile information for each type of certificate can be found in the *NSS PKI Certificate Profiles Specification* [NSS PKI PROF].

## 1.1 OVERVIEW

The NSS PKI CP is the policy under which the NSS PKI operates. This document will be reviewed and updated as described in Section 9.12.1.

This CP defines the creation and management of certificates that comply with the *International Telecommunications Union (ITU) X.509: Information Technology - Open Systems Interconnection - The Directory: Public-Key and Attribute Certificate Frameworks X.509 Version 3 Public Key Certificates* [ITU X.509] for use in applications requiring communication between networked computer-based systems. Such applications include, but are not limited to, signature of electronic mail; encryption of information; and authentication to networks, web servers or other applications. This CP is consistent with the *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* [RFC 3647].

A bibliography of referenced publications is included as Appendix A; a list of acronyms is provided as Appendix B; and, a glossary of terms is provided as Appendix C.

### 1.1.1 Certificate Policy

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

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

### 1.1.2 Relationship between the Certificate Policy and the Certification Practice Statement

This NSS PKI CP states the requirements for issuing and managing certificates that Relying Parties can use in making decisions regarding what assurance they can place in a certificate issued by a NSS PKI CA. The Certification Practice Statement (CPS) states how a NSS PKI member establishes and maintains that assurance. Each CA that issues certificates under this policy shall have a corresponding approved CPS detailing its operating practices. Agencies that use the services of a CA operated by a different agency are subject to the CPS for the CA that is providing certificates. Registration Authorities (RA) and Trusted Agents (TA) that support certificate issuance and management processes are subject to the CPS for the CA that is providing certificates. RAs and TAs may also have a distinct Registration Practices Statement (RPS) that details the specific policies and processes under which they operate.

### 1.1.3 Scope

This CP applies to CA Systems (CAS) that issue certificates that assert this policy and all certificates issued to CAs, other CAS components, named individuals, roles, and systems or devices that assert a NSS PKI Certificate Policy OID (see Section 1.2). This CP also applies to the individuals responsible for these certificates and persons operating the NSS PKI.

### 1.1.4 Interoperation with CAs Issuing Under Different Policies

Interoperability with CAs that issue certificates under different policies that assert different policy OIDs, may be achieved through policy mapping and cross-certification. All requirements identified in this CP will be considered as part of any cross-certification decision. This CP accommodates cross-certification with CNSS member legacy NSS PKIs. By 1 October 2012, all legacy NSS PKIs must have established a Subordinate CA under the NSS PKI.

## 1.2 DOCUMENT NAME AND IDENTIFICATION

The official title of the CP is the “*Instruction for National Security Systems (NSS) Public Key Infrastructure (PKI) X.509 Certificate Policy Under CNSS Policy No. 25*.”

The NSS PKI CP defines five Certificate Policies. Each Certificate Policy has an OID, to be asserted in certificates issued by CAs that comply with the stipulations related to that policy. The NSS PKI Certificate Policy OIDs are registered under the National Institute of Standards and Technology (NIST) Computer Security Objects Register (CSOR) arc as follows:

id-cnss-policies:: = {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) pki(2) cert-policy(1) cnss(21)}

| | |
|---|---|
| *id-CNSS-software* | ID::={id-CNSS-policies (1)} |
| *id-CNSS-hardware* | ID::={id-CNSS-policies (2)} |
| *id-CNSS-device* | ID::={id-CNSS-policies (3)} |
| *id-CNSS-peer-software* | ID::={id-CNSS-policies (4)} |
| *id-CNSS-peer-hardware* | ID::={id-CNSS-policies (5)} |

The stipulations presented in this CP apply to all policies unless otherwise noted. CAs that do not meet the stipulations presented in this CP may be cross certified using the *id-CNSS-peer-software* or *id-CNSS-peer-hardware* OIDs as specified in Section 3.2.6.

This CP is the authoritative source for the definition and assignment of NSS PKI Certificate Policy OIDs.

## 1.3 PKI PARTICIPANTS

The following sections introduce the entities that participate in the NSS PKI. Responsibilities, qualifications, and additional controls for individuals designated as holding a trusted role are described in detail in Sections 5.2 and 5.3.

### 1.3.1 CNSS Policy Management

The NSS PKI is managed by the CNSS Policy Management Authority (PMA) as assisted by the NSS PKI Member Governing Body.

#### *1.3.1.1 NSS PKI Policy Management Authority*

The NSS PKI PMA has the following responsibilities:

- Approve this CP, including changes recommended by the NSS PKI Member Governing Body
- Approve the issuance of certificates from the Root CA to Intermediate or Subordinate CAs
- Approve CPSs recommended by the NSS PKI Member Governing Body as compliant with this CP
- Approve the establishment of trust relationships with external PKIs that offer appropriately comparable assurance to one or more certificate policies as set forth in this CP as recommended by the NSS PKI Member Governing Body
- Act as final authority for dispute resolution among the NSS PKI Member Governing Body members to include compliance audit appeals

The PMA for the NSS PKI is the Director, National Security Agency (DIRNSA).

#### *1.3.1.2 NSS PKI Member Governing Body*

All Federal Government Departments and Agencies that require or rely on certificates issued by the NSS PKI shall participate in the NSS PKI Member Governing Body. The NSS PKI Member Governing Body has the following responsibilities:

- Maintain this CP, including evaluation of changes requested by CNSS member agencies and make recommendations to the PMA
- Establish the NSS PKI
- Review requests for the issuance of Intermediate or Subordinate CA certificates and provide recommendations for issuance to the PMA
- Perform compliance analysis of CPSs to determine if they meet the requirements of this CP and make recommendations to the NSS PKI PMA
- Perform review of external PKIs, including policy mapping, to determine if they offer appropriately comparable assurance to one or more certificate policies as set forth in this CP and make recommendations to the PMA
- Review and approve the results of compliance audits of member entities (see Section 8)

The authorities and operating procedures for the NSS PKI Member Governing Body (MGB) are contained in the NSS PKI MGB Charter and By-Laws.

#### *1.3.1.3 Agency NSS PKI Management Authority*

Agencies that operate a CA under this policy shall establish an Agency NSS PKI Management Authority (ANMA). The ANMA is responsible for all aspects of management of the NSS PKI program for that agency and is responsible for participating in the NSS PKI Member Governing Body. Agencies may establish other organizational bodies under the oversight of the ANMA to perform functions relating to CA governance or operations. Each ANMA shall prepare and submit a CPS governing each CA subordinate to the NSS PKI Root CA that conforms to the requirements of the NSS PKI CP.

Agencies may choose to implement RPSs. If so, the ANMA shall perform a compliance analysis of RPSs to determine if they meet the requirements of this CP and the supporting Agency's CPS.

#### *1.3.1.4 Agency NSS PKI Point of Contact*

Agencies that do not operate a CA under this policy, but who obtain certificates from a Common Services CA operated under this policy shall designate a Point of Contact (POC) to serve as the liaison for that agency to the NSS PKI Member Governing Body and to the ANMA that is providing CA services. The Agency NSS PKI POC is responsible for all aspects of management of the NSS PKI program for that agency and is responsible for participating in the NSS PKI Member Governing Body.

If the Agency operating the Common Services Provider CA uses RPSs, each participating Agency who performs RA functions shall prepare and submit an RPS to the ANMA of the Agency operating the Common Services Provider CA.

### 1.3.2 Certification Authority System

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

- The certificate manufacturing and issuance process
- Publication of certificates (as applicable)
- Revocation of certificates
- Publication of CRLs
- Escrow of private keys associated with encryption certificates
- Generation and destruction of CA signing keys
- Ensuring that all aspects of the CAS services, operations, and infrastructure related to certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP

The division of Subscriber registration responsibilities between the CAS, RA, and TA may vary among implementations of this CP. CAs are ultimately responsible for ensuring that all certificates they sign are generated and managed in accordance with this policy, and shall ensure that certificate generation, management, and revocation functions are performed only by those who understand the associated Certificate Policy OID requirements, and who are obligated to meet them.

CAS is a broad term that covers all components defined in this section, including the CA itself, the Audit System, the Key Escrow System (KES), and the Certificate Status Server (CSS); as well as the individuals who are part of the CAS operations staff. Unless expressly stated otherwise, CAS requirements are imposed on all CAS components.

#### *1.3.2.1 Certification Authority*

The CA processes certificate requests and issues certificates. In addition, the CA processes certificate revocation requests and issues CRLs.

The NSS PKI includes three types of CAs: Root, Intermediate, and Subordinate. The following table summarizes the entities that are issued certificates by each type of CA.

**Table 1-1: CA Types**

| CA Type | Entities Issued Certificates |
|---|---|
| Root CA | • Root CA signing certificate<br>• Components of the Root CAS<br>• Individuals holding trusted roles on the Root CAS<br>• Components of Intermediate or Subordinate CASs (e.g., certificates to a Subordinate CA or CSS)<br>• External CAs that have been approved by the NSS PKI PMA (i.e., cross certificates) |
| Intermediate CA | • Components of the Intermediate CAS other than its own signing certificate<br>• Individuals holding trusted roles on the Intermediate CAS<br>• Components of other Intermediate or Subordinate CASs (e.g., certificates to a Subordinate CA or CSS) |
| Subordinate CA | • Components of the Subordinate CAS other than its own signing certificate<br>• Individuals holding trusted roles on the Subordinate CAS<br>• Subscribers |

#### *1.3.2.2 Audit System*

The Audit System is used to collect security audit data for the CA, KES, and CSS. The Audit System may be external to the CA or other system or may be operated as an internal component. The Audit System may also be a single system, or distributed across multiple systems. Requirements for the Audit System are detailed in Section 5.4.

#### *1.3.2.3 Key Escrow System*

The KES stores private keys associated with encryption certificates, which are necessary for the recovery of encrypted data. The KES may be external to the CA or may be operated as an internal component. It provides a mechanism for obtaining a copy of the escrowed key in order to decrypt the data encrypted using the associated public key.

#### *1.3.2.4 Certificate Status Server*

The NSS PKI or any CAS operated under the NSS PKI may optionally include an authority that provides status information about certificates on behalf of the CA through online transactions. In particular, a CAS may include an Online Certificate Status Protocol (OCSP) responder. Such an authority is termed a CSS. The operations of a CSS designated as an authoritative source of revocation information by the NSS PKI are considered within the scope of this CP. The NSS PKI designates a CSS as authoritative by issuing the CSS a certificate from the CA for which it will sign responses or by listing the CSS in end entity certificates as an authoritative source (e.g., the CSS is identified in the *authorityInformationAccess* (AIA) extension). A CSS that is not designated as authoritative (i.e., the CSS is not listed by the CA in the end entity certificate as authoritative and is not issued a certificate by the CA for which it provides responses) is not considered part of the NSS PKI and is not subject to the stipulations of this CP.

#### *1.3.2.5 CAS Operations Staff*

CAS components are operated and managed by individuals holding trusted roles. Specific responsibilities for these roles, as well as requirements for separation of duties, are described in Section 5.2. CAS Operations Staff are designated as holding a trusted role.

CAS Operations Staff that perform RA Officer Roles when verifying information for RA Officers are acting as RA Officers. As a result, requirements identified for RA Officers also apply to these individuals.

### 1.3.3 Registration Authority

An RA is an entity authorized by the CAS to collect, verify, and submit information provided by potential Subscribers which is to be entered into public key certificates. The term RA refers to hardware, software, and individuals that collectively perform this function. Unless expressly stated otherwise, RA requirements are imposed on all RA components of the NSS PKI. RA operations shall be performed in accordance with a CPS approved by the NSS PKI PMA. RA functions may be included in a single CPS, which also governs CAS operations, or may be defined in a separate RPS. The RA is responsible for the following:

- Control over the registration process
- The identification and authentication process

#### *1.3.3.1 RA System*

The RA System includes hardware and software that is used to support the CAS in collecting and formatting information that is to be used in certificate issuance, certificate revocation, and key recovery. External databases that are used to support the verification of Subscriber or Requestor information are not considered part of the RA System.

#### *1.3.3.2 RA Operations Staff*

RA components are operated and managed by individuals holding trusted roles. Specific responsibilities for these roles, as well as requirements for the separation of duties, are described in Section 5.2. RA Operations Staff are designated as holding a trusted role.

#### *1.3.3.3 RA Officer*

An individual who is responsible for any of the duties of certificate issuance, certificate revocation, or key recovery is designated as an RA Officer. Duties may be performed by the same individual, or may be separated across different roles. RA Officers are designated as holding a trusted role.

### 1.3.4 Trusted Agent

A TA is an individual explicitly aligned with one or more RA Officers who has been delegated the authority to perform a portion of the RA function (e.g., a TA may perform identity proofing of certificate applicants for a requestor who cannot appear in person to an RA Officer). A TA does not have privileged access to CAS components to authorize certificate issuance, certificate revocation, or key recovery. Instead, the TA provides information to the RA in a secure fashion. An RA Officer shall approve requests submitted by TAs. TAs are designated as holding a trusted role.

### 1.3.5 Subscriber

A Subscriber is the entity whose name appears as the subject in a certificate. The NSS PKI supports issuing certificates to three types of Subscriber: Name, Role, and System or Device. Unless otherwise specified, requirements for Subscriber apply to all three types. Certificates shall also have a person who is responsible for the private key associated with a certificate, and who asserts that the certificate and associated private key are being used in accordance with this CP, known as the PKI Sponsor. Each of the types of Subscriber has an associated PKI Sponsor. The following table shows the PKI Sponsor for each type of Subscriber.

**Table 1-2: Subscriber Types**

| Subscriber Type | PKI Sponsor |
|---|---|
| Name | Individual named in the certificate |
| Role | Individual authorized to use certificate or designated individual responsible for management of Role certificates |
| System or Device | Designated individual responsible for system or device keys |

CASs are sometimes technically considered Subscribers in a NSS PKI. However, the term Subscriber as used in this document refers only to those entities that request certificates for uses other than signing and issuing certificates or certificate status information.

#### *1.3.5.1 Name Subscriber*

Name certificates contain an individual name as the subject. Name certificates are tightly coupled with the individual named in the certificate. Name certificates are issued to Federal Government employees, contractors, and affiliates. The PKI Sponsor for a Name certificate is the individual named in the certificate.

#### *1.3.5.2 Role Subscriber*

Role certificates contain a role, group, or organization name as the subject; they do not contain the name of an individual in the *Distinguished Name* (DN) field. The PKI Sponsor for a Role certificate is an individual who shall be explicitly responsible for managing access to the private key associated with the certificate. In addition, technical or procedural controls shall be implemented to document and manage who has access to the private key associated with the certificate.

#### *1.3.5.3 System or Device Subscriber*

System or Device certificates contain a system or device name as the subject. Examples of systems or devices are workstations, guards, firewalls, routers, web server, database server, and other infrastructure components. The PKI Sponsor for a System or Device certificate is an individual who shall be explicitly responsible for managing access to the private key associated with the certificate.

### 1.3.6 Relying Party

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

- The identity and status of an individual, role, or system or device
- The integrity of a digitally signed message
- The identity of the creator of a message
- Confidential communications with the Subscriber

A Relying Party is the entity that relies on the validity of the binding of the Subscriber's name to a public key. A Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. A Relying Party may use information in the certificate (such as Certificate Policy OID identifiers) to determine the suitability of the certificate for a particular use.

Relying Parties may base the reliance they choose to place on a certificate on the factors such as the amount and type of inherent risk of an activity, the consequence of failure, and the use of risk mitigation controls.

### 1.3.7 Other Participants

CASs and RAs operating under this CP may require the services of other security, community, and application authorities, such as compliance auditors. These authorities, their services, and the mechanisms used to support their services shall be identified. An entity with privileged access to the CAS or RA system, or with the ability to approve or reject issuance of a certificate, approve revocation of a certificate, or approve removal of a certificate from hold on the CAS or RA system, shall be designated as holding a trusted role, and shall meet the personnel controls identified in Section 5.3.

## 1.4 CERTIFICATE USAGE

The NSS PKI can support the following security services: confidentiality, integrity, authentication, and technical non-repudiation. The NSS PKI supports the authentication, integrity, and technical non-repudiation security services through digital signatures, and the confidentiality security service through encryption. These basic security services support the long-term integrity of application data, but by themselves may not provide a sufficient integrity solution for all application circumstances.

### 1.4.1 Appropriate Certificate Uses

Certificates issued under this policy asserting *id-CNSS-software*, *id-CNSS-hardware*, or *id-CNSS-device* shall only be used to protect SECRET or below classified information within U.S. SECRET networks or information systems. Peer OIDs (*id-CNSS-peer-software* and *id-CNSS-peer-hardware*) will be assessed against ability to protect SECRET data on SECRET networks only.

### 1.4.2 Prohibited Certificate Uses

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

## 1.5 POLICY ADMINISTRATION

### 1.5.1 Organization Administering the Document

The NSS PKI PMA is responsible for all aspects of this CP.  See Section 1.3.1.1 for a description of the NSS PKI PMA.

### 1.5.2 Contact Person

Questions regarding this CP should be directed to:

CNSS Secretariat
National Security Agency
9800 Savage Road, Ste 6716
Fort George G. Meade, MD 20755-6716

### 1.5.3 Person Determining CPS Suitability for the Policy

The NSS PKI PMA shall determine the suitability of any CPS to this policy as recommended by the NSS PKI Member Governing Body.

### 1.5.4 CPS Approval Procedures

CASs operating under this policy are required to meet all facets of this policy.  CPSs shall be submitted to the NSS PKI Member Governing Body for compliance analysis with this CP.  The NSS PKI Member Governing Body shall perform a compliance analysis study culminating in a written report to the NSS PKI PMA that provides a summary of areas in which the CPS does or does not comply with this CP.  All CASs and RAs shall have a PMA-approved CPS and conduct an initial compliance audit showing that they meet all CP and CPS requirements prior to commencing operations.  See Section 8 for more information regarding the initial compliance audit.

All RA Officers and TAs shall operate either under a PMA-approved CPS or an ANMA-approved RPS.  RPSs shall be submitted to the ANMA for the Agency operating the CA that the RA or TA supports.  The ANMA shall perform a compliance analysis study to ensure that the RPS complies with all relevant aspects of the ANMA's approved CPS.

### 1.5.5 Waivers

Waivers shall not be granted under any level of assurance.  Variation in CAS and RA practices shall either be deemed acceptable under a current Certificate Policy OID, a change shall be requested to the policy, or a new Certificate Policy OID shall be established for the non-compliant practice.

## 1.6 DEFINITIONS AND ACRONYMS

See Appendix B and Appendix C.

# 2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

## 2.1 REPOSITORIES

The NSS PKI Member Governing Body intends to use a central repository providing CA certificates and CRLs that supports overall NSS PKI operations with both Hyper Text Transfer Protocol (HTTP) and Lightweight Directory Access Protocol (LDAP) interfaces. The central repository function may consist of one or more repositories to support overall NSS PKI operations at the discretion of the NSS PKI Member Governing Body or the PMA. The central repository shall be operational 24 hours a day, 7 days a week with a minimum of 99% availability overall per year and scheduled down-time not to exceed 0.5% annually. The central repository shall collect necessary information from the agency repositories.

Each agency that operates a CA shall maintain one or more repositories that support HTTP or LDAP to provide CA certificates and CRLs. Agency repositories shall be operational 24 hours a day, 7 days a week with a minimum of 95% availability overall per year.

Each member agency shall maintain a repository that collects information from the central repository for use by systems on that agency’s network.

## 2.2 PUBLICATION OF CERTIFICATION INFORMATION

The NSS PKI Member Governing Body shall publish this CP to the NSS PKI web site. The NSS PKI shall also publish notification of the issuance of cross certificates along with text from the cross certification Memorandum of Agreement (MOA) specifying any deviance in operations from requirements of this CP.

Each CA shall publish certificates needed to verify certificate and CRL signatures, any certificates used to sign CSS responses, and any cross certificates issued by the CA. Each CA shall also publish the most recently issued CRL.

CA information shall be made available to the central repository; the central repository shall make all necessary information available to member agency repositories.

This CP makes no requirement for the publication of Subscriber certificates.

## 2.3 TIME OR FREQUENCY OF PUBLICATION

CRLs shall be published to Agency repositories as specified in Section 4.9.7. All information published to any repository shall be published promptly after such information becomes available to a CA. The NSS PKI central repository shall obtain information from Agency repositories for Agencies that operate a CA within six hours of publication of that information to the Agency repository. Member agencies that rely on NSS PKI certificates shall obtain information from the central repository at least every six hours. Requirements for posting of revocation data are contained in the Section 4.9.7 and 4.9.8.

## 2.4 ACCESS CONTROLS ON REPOSITORIES

Repository information shall be protected from unauthorized modification, deletion, and disclosure. Each NSS PKI CAS shall adequately protect any repository information not intended for public dissemination; and shall not make Subscriber certificates automatically available on any public facing repository.

Repositories that contain sensitive information shall have access controls in place commensurate with the sensitivity of the information. Sections 9.3, 9.4, and 9.5 detail what information in the repository shall be exempt from automatic availability and to whom, and under what conditions the ANMA may make restricted information available.

For remote access protection when modifying or deleting repository information, or when accessing sensitive information requiring controls as required above, client authentication shall be employed using a NSS PKI certificate commensurate with the repository data.

# 3 IDENTIFICATION AND AUTHENTICATION

## 3.1 NAMING

### 3.1.1 Types of Names

The NSS PKI Root CA, Intermediate CAs, and Subordinate CAs shall only generate and sign certificates that contain a non-null subject DN and issuer DN. Certificates may also include alternative name forms (see Section 7.1.4).

For Subordinate CAs, the following rules apply:

- All certificates shall use the DN name form for the *issuerName* and *subjectName* fields
- Other name types may be included in other fields
- Subscribers shall have DNs assigned to them through their agency. For Subscribers obtaining certificates from a Common Services Provider CA, naming structures shall be determined between the Subscriber Agency POC and the ANMA for the Common Services Provider CA
- All certificates issued to end entities shall include a non-null subject DN, and may include alternative name forms

### 3.1.2 Need for Names to be Meaningful

Names used within the NSS PKI shall identify the entity to which they are assigned in a meaningful way. The RA shall ensure that an affiliation exists between the Subscriber and any organization identified by any component of any name in its certificate.

The common name shall represent the Subscriber. For Name and Role certificates, the common name shall be easily understandable for humans. For Name Certificates, this will typically be a legal name. For Role Certificates, this will typically be the formally recognized name of the role, group, or organization. For System or Device Certificates, this typically will be a fully qualified domain name, an Internet Protocol (IP) address, a model name and serial number, or an application name.

A CA asserting one or more of the Certificate Policy OIDs specified in this CP shall only sign certificates with subject names from within the name-space approved by the NSS PKI Member Governing Body, or cross certificates as approved by the PMA. In the case where one CA issues a CA certificate to a Subordinate CA, the issuing CA shall impose restrictions on the name space authorized to the Subordinate CA, which are at least as restrictive as its own name constraints.

### 3.1.3 Anonymity or Pseudonymity of Subscribers

The NSS PKI shall not issue anonymous certificates. CA certificates shall not contain anonymous or pseudonymous identities. A Subordinate CA may issue pseudonymous certificates (e.g., Role Certificates).

### 3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting name forms shall use the appropriate standard (e.g., *Internet Engineering Task Force (IETF) RFC 5322 Internet Message Format* [RFC 5322] for Internet email addresses). The applicable certificate profile (see Section 7.1) will contain the rules for interpreting that name form.

### 3.1.5 Uniqueness of Names

The NSS PKI Member Governing Body shall enforce subject name uniqueness across the NSS PKI. Each CA shall enforce name uniqueness within its allocated name space among both current and past Subscribers. If more than one CA issues certificates within the same name space, the ANMA shall enforce name uniqueness across all CAs using that name space. When the Root CA issues a cross certificate to another CA, the NSS PKI Member Governing Body shall ensure that name uniqueness requirements are maintained.

The RA Officer shall investigate and, if necessary, recommend the correction for any name collisions brought to its attention. If appropriate, the RA Officer shall coordinate with and defer to the appropriate naming authority.

### 3.1.6 Recognition, Authentication and Role of Trademarks

A CA shall not knowingly issue a certificate that contains a trademark in the name. A CA shall not knowingly issue a certificate including a name that a court of competent jurisdiction has determined infringes the trademark of another. A CA is not subsequently required to issue that name to the rightful owner if it has already issued one sufficient for identification. CASs and RAs are not obligated to research trademarks or resolve trademark disputes.

## 3.2 INITIAL IDENTITY VALIDATION

### 3.2.1 Method to Prove Possession of Private Key

In all cases where the Subscriber named in a certificate generates its own keys, the Subscriber or PKI Sponsor shall be required to prove possession of the private key, which corresponds to the public key in the certificate request, to the CAS or RA. In the case where keys are generated directly on a token, or in a key generator that benignly transfers the key to the token under the direct control of the CAS, proof of possession is not required.

If the PKI Sponsor is not in possession of the token when the key is generated, then the token shall be delivered to the PKI Sponsor via an accountable method (see Section 6.1.2).

### 3.2.2 Authentication of Organization Identity

Organization information contained in certificates shall be verified. For specific requirements for verification of Role Subscriber information, see Section 3.2.3.2.

### 3.2.3 Authentication of Individual Identity

The CAS or RA shall verify the PKI Sponsor applicant’s identity information.

#### *3.2.3.1 Authentication for Name Subscribers*

The RA shall authenticate the identity and the specified attributes for Name Subscribers through all of the following mechanisms prior to initial certificate issuance:

- **Identity:** The applicant shall appear in-person before an RA Officer or TA and present either a valid Personal Identity Verification (PIV) card issued in compliance with *Federal Information Processing Standard (FIPS) 201, Personal Identity Verification (PIV) of Federal Employees and Contractors* [FIPS 201] or two forms of identity source documents in original form. The identity source documents shall come from the list of acceptable documents included in *OMB No. 1615-004, Form I-9, Employment Eligibility Verification* [FORM I-9]. At least one document shall be a valid State or Federal government-issued picture identification (ID).

  The RA Officer or TA shall visually inspect the identification documents and authenticate them as being genuine and unaltered. In addition, the RA Officer or TA shall electronically verify the authenticity of the source document, when such services are offered by the issuer of the source document. When electronic verification is not offered, the RA Officer or TA shall use other available tools to authenticate the source and integrity of the identity source documents.
- **Citizenship:** The RA Officer or TA shall determine the citizenship of the applicant through an authoritative source (e.g., security database) or through presentation of a passport, birth certificate, or U.S. Government issued identification that denotes citizenship.
- **Clearance:** The RA Officer or TA shall ensure that the applicant possesses a minimum of a current SECRET clearance. The clearance shall be determined through an authoritative source (e.g., security database).
- **Account:** The RA Officer or TA shall ensure the applicant possesses an account on an accredited U.S. SECRET level information system or network.

The RA Officer or TA shall sign a declaration acknowledging that they have verified the identity and any attributes in accordance with this policy.

Electronic authentication of a valid Identity certificate For Name Subscribers may be accepted as proof of identity, citizenship, clearance, and account for the issuance of Signature or Encryption certificates if all of the following are true:

- The Certificate Policy OID of the new certificate is the same as that of the Identity certificate
- The DN of the new certificate is identical to the DN of the Identity certificate
- Information in the new certificate that could be used for authorization is identical to that of the Identity certificate
- The expiration date of the new certificate is no later than the next required in-person authentication date associated with the Identity certificate
- The in-person authentication date associated with a new certificate is no later than the in-person authentication date associated with the Identity certificate

An RA Officer or TA may accept digitally signed electronic requests for renewal, re-key, or modification of certificates from the Name Subscriber in accordance with the requirements in

Sections 4.6, 4.7, and 4.8. Requests for certificate modification requiring presentation of appropriate documentation to re-establish authorization shall only be accepted in accordance with the requirements in Section 4.8.

#### *3.2.3.2 Authentication for Role Subscribers*

Requests for Role Certificates shall be accompanied by documentation provided by the PKI Sponsor describing the role, the users of the role, and other necessary information. The information required shall be sufficient to determine the validity of the role. The RA shall authenticate the identity of the PKI Sponsor and the specified attributes for Role Certificate through the following mechanisms:

- **Role:** The RA shall verify the approved existence of the role via organizational processes
- **Authority:** The RA shall verify the authority of the PKI Sponsor to request a Role Certificate via organizational processes
- **Identity:** The RA shall verify that the PKI Sponsor possesses a valid NSS PKI issued Name certificate, and that the PKI Sponsor has a process to ensure that each Role Certificate user possesses a valid Name Certificate
- **Attributes:** The RA shall verify any attributes asserted by the Role Certificate via organizational processes

The PKI Sponsor shall be accountable for the private key associated with the Role Certificate, and shall acknowledge and accept overall responsibility for the use of the Role Certificate and protection of its associated private key. The PKI Sponsor shall ensure that each individual who has access to the private key associated with the Role Certificate at any time possesses a valid NSS PKI Name Certificate. The PKI Sponsor shall ensure that no individual continues to have access to the private key associated with the Role Certificate after leaving the Role.

The RA Officer or TA shall sign a declaration acknowledging that they have verified the identity and any attributes in accordance with this policy.

#### *3.2.3.3 Authentication for System or Device Subscribers*

Requests for System or Device Certificates shall be accompanied by documentation provided by the PKI Sponsor identifying the System or Device, and other necessary information. The RA shall authenticate the identity of the PKI Sponsor and the specified attributes for System or Device Certificate through the following mechanisms:

- **System or Device:** The RA shall verify the approved existence of the System or Device via organizational processes
- **Authority:** The RA shall verify the authority of the PKI Sponsor to request a System or Device Certificate via organizational processes
- **Identity:** The RA shall verify that the PKI Sponsor possesses a valid NSS PKI issued Name Certificate
- **Attributes:** The RA shall verify any attributes asserted by the Role Certificate via organizational processes

The PKI Sponsor shall be accountable for the System or Device Certificate, and shall acknowledge and accept overall responsibility for the use of the System or Device Certificate and protection of the associated private key.

The RA Officer or TA shall sign a declaration acknowledging that they have verified the identity and any attributes in accordance with this policy.

### 3.2.4 Non-Verified Subscriber Information

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

### 3.2.5 Validation of Authority

Before issuing a certificate that contains explicit or implicit authority, the CAS shall validate that authority as described in Section 3.2.3.

### 3.2.6 Criteria for Interoperation

This CP shall form the basis for determining the criteria for interoperation. However, the decision to establish formal trust relationships (e.g., cross certification) for the NSS PKI with an external PKI shall reside with the PMA. Prior to the issuance of a cross certificate, an MOA shall be executed between the NSS PKI PMA and the PMA of the requesting CAS that indicates the terms of the cross-certification agreement.

CAs that do not fully comply with all requirements identified in this CP shall only be cross-certified using the *id-CNSS-peer-software* or *id-CNSS-peer-hardware* OIDs. Discrepancies between the operations of a cross-certified CAS and the requirements identified in this CP shall be documented in the MOA. The NSS PKI web site shall identify how Relying Parties can obtain copies of MOAs.

## 3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

### 3.3.1 Identification and Authentication for Routine Re-Key

See Section 4.7 for certificate re-key requirements.

### 3.3.2 Identification and Authentication for Re-Key After Revocation

If a certificate has been revoked due to compromise, termination, or change to the identity or status of an individual, role, or of the system or device, identity shall always be re-established through the initial registration process in accordance with Sections 3.2.2 and 3.2.3.

## 3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

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

## 3.5 IDENTIFICATION AND AUTHENTICATION FOR KEY RECOVERY REQUEST

### 3.5.1 Subscriber Request

PKI Sponsors are authorized to request the recovery of their own escrowed keys.

For automated self-recovery of private keys for Name certificates, the PKI Sponsor shall be authenticated using a valid certificate asserting the same policy as that of the certificate associated with the escrowed key.

Alternatively, the PKI Sponsor shall establish his or her identity to an RA, either through the use of a valid certificate asserting the same policy as that of the certificate associated with the escrowed key, or using the procedures specified in Section 3.2.3.1 for authenticating identity. If the authentication is not based on digital signatures that can be verified using the public key certificates, the RA Officer or TA shall personally verify the identity of the PKI Sponsor prior to initiating the key recovery request.

If a TA is performing the requestor validation, the TA shall establish his or her identity to the RA Officer based on a digital signature that can be verified using the public key certificate of the TA. TA certificates that assert the *id-CNSS-software* OID shall only be accepted for recovery of Subscriber certificates that assert the *id-CNSS-software* OID. TA certificates that assert the *id-CNSS-hardware* OIDs may be accepted for recovery of Subscriber certificates that assert any OID.

### 3.5.2 Third Party Request

Entities other than PKI Sponsors may request recovery of escrowed key material. All requests shall be coordinated through an RA Officer or TA, who shall validate the authorization of the requestor in consultation with organization management and/or legal counsel, as appropriate.

The requestor shall establish his or her identity to the RA Officer or TA, either through the use of a valid certificate asserting the same policy as that of the certificate associated with the escrowed key, or using the procedures specified in Section 3.2.3.1 for authenticating identity. The RA Officer or TA shall personally verify the identity and authority of the requestor prior to initiating the key recovery request.

If a TA is performing the requestor validation, the TA shall establish his or her identity to the RA Officer based on a digital signature that can be verified using the public key certificate of the TA. TA certificates that assert the *id-CNSS-software* OID shall only be accepted for recovery of Subscriber certificates that assert the *id-CNSS-software* OID. TA certificates that assert the *id-CNSS-hardware* OIDs may be accepted for recovery of Subscriber certificates that assert any OID.

# 4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

## 4.1 CERTIFICATE APPLICATION

This CP identifies the minimum requirements and procedures that are necessary to support trust in the NSS PKI, and to minimize imposition of specific implementation requirements on CASs, RAs, TAs, PKI Sponsors, and Relying Parties.

All communications between CAS, RA, and TA components shall be authenticated and protected from modification using mechanisms commensurate with the requirements of the data to be protected by the certificates being issued. Any electronic transmission of shared secrets shall be protected (e.g., encrypted) using means commensurate with the requirements of the data to be protected by the certificates being issued.

### 4.1.1 Who Can Submit a Certificate Application

Certificate applications may be submitted to the CAS by the PKI Sponsor or an RA. TAs may only assist in the submission of certificate applications in the presence of the PKI Sponsor or RA. TAs shall never be in possession of a private key associated with the public key in a certificate request.

An application for a cross certificate from an external PKI shall be submitted by an authorized representative of the external PKI directly to the NSS PKI Member Governing Body or indirectly through an ANMA. Cross certificates shall only be issued by the CNSS Root CA, Intermediate CA, or Subordinate CA upon authorization by the NSS PKI PMA.

### 4.1.2 Enrollment Process and Responsibilities

The certificate application process shall provide sufficient information to establish the identity and authority of the requestor, verify any role or authorization information requested for inclusion in the certificate, generate a public/private key pair, ensure that the applicant possesses the private key associated with the public key in the certificate, and ensure that the applicant formally acknowledges and accepts responsibility for the certificate and associated private key. These steps may be performed in any order that is convenient for the NSS PKI authorities and applicants, and that do not defeat security; but all must be completed prior to certificate issuance.

Requests by CAs for CA certificates from the CNSS Root CA shall be submitted to the NSS PKI Member Governing Body using the contact provided in Section 1.5.2. A CPS conforming to the format in [RFC 3647] shall accompany requests. The NSS PKI Member Governing Body shall evaluate the submitted CPS for acceptability and make a recommendation to the PMA. The Root CA shall not issue a CA signing certificate until authorized by the PMA.

Requests by CAs for CA signing certificates from an Intermediate or Subordinate CA shall be submitted to the ANMA of the Agency operating the Intermediate or Subordinate CA. The request shall indicate that the CA will be operating under an already approved CPS. The ANMA shall ensure that the CAS is in scope of the CPS and make a determination regarding issuance of the CA certificate.

## 4.2 CERTIFICATE APPLICATION PROCESS

### 4.2.1 Performing Identification and Authentication Functions

Upon receiving the request, the RA shall perform the following:

- Establish, authenticate, and record identity of the applicant as described in Section 3.2
- Verify the authority of the applicant to obtain the certificate and the integrity of the information in the certificate request
- Build the certificate and approve the signature of the certificate by the CA, if all requirements have been met
- Ensure the PKI Sponsor formally acknowledges and accepts responsibilities associated with holding the certificate through signing an acknowledgement of responsibilities form

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 RA's satisfaction.

The RA shall be ultimately responsible for verifying that the information to be included in the certificate is correct and accurate. When information has been submitted by a TA, TAs shall verify all information prior to submission, and the RA shall verify the identity of the TA, the authority of the TA, and the integrity of the information submitted by the TA. Information and attributes shall be verified via those offices or roles that have authority to assign the information or attribute. RAs and TAs shall establish relationships with these offices or roles to include this information in any certificate prior to approval.

### 4.2.2 Approval or Rejection of Certificate Applications

The CAS, RA, or TA may reject certificate application for various reasons such as incomplete or inaccurate information, lack of authorization to provide a certificate to the PKI Sponsor, inability to verify information to be included in the certificate, or technical errors such as failure to escrow the private key associated with an encryption certificate. If an application is rejected, the RA Officer or TA shall work with the appropriate parties to resolve the problem.

A certificate application is not considered accepted until the CA has accepted the application and issued a certificate.

### 4.2.3 Time to Process Certificate Applications

The RA or TA shall identify and authenticate the PKI Sponsor not more than 30 days prior to certificate issuance. If more than 30 days have passed between in-person identity proofing and certificate acceptance, the RA or TA shall re-confirm the identity of the PKI Sponsor prior to certificate issuance.

## 4.3 CERTIFICATE ISSUANCE

### 4.3.1 CA Actions during Certificate Issuance

Either an RA or the CAS shall ensure that the certificate request has been authenticated and validated, ensure that the public key is bound to the correct Subscriber, and obtain a proof of possession of the private key. The CAS shall authenticate the RA and the integrity of the request data received from the RA; then generate a certificate and provide the certificate to the PKI Sponsor.

### 4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The CAS or RA shall notify the PKI Sponsor of certificate issuance.

## 4.4 CERTIFICATE ACCEPTANCE

### 4.4.1 Conduct Constituting Certificate Acceptance

The PKI Sponsor's formal acknowledgement and acceptance of responsibilities associated with holding the certificate through signing an acknowledgement of responsibilities form shall constitute acceptance of the certificate. The PKI Sponsor signature shall be collected before a CAS allows a Subscriber to make effective use of its private key. For certificate re-key, renewal, or modification, the PKI Sponsor's request to obtain a new certificate and subsequent failure to object to the certificate or its contents shall constitute acceptance of the certificate.

### 4.4.2 Publication of the Certificate by the CA

See Section 2.2.

### 4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The NSS PKI PMA and NSS PKI Member Governing Body shall be notified whenever a CA operating under this policy issues a CA certificate.

## 4.5 KEY PAIR AND CERTIFICATE USAGE

### 4.5.1 Subscriber Private Key and Certificate Usage

The use of the private key shall be limited in accordance with the *Key Usage* extension in the associated certificate. If the *Extended Key Usage* extension is present and implies any limitation on the use of the private key, those constraints shall also be observed.

A Subscriber shall not use a private key associated with an Identity, Code Signing, Content Signing, or System or Device certificate after the associated certificate has expired or been revoked. A Subscriber may continue to use a private key associated with an Encryption certificate after the associated certificate has expired or been revoked solely to decrypt previously encrypted information.

Each NSS PKI member agency that supports Role Subscribers shall develop internal policies and procedures for the use of Role Certificates and protection of the associated private keys for its specific operational environment.  PKI Sponsors shall maintain a list of individuals with access to the private key of Role certificates at any given date/time.

### 4.5.2 Relying Party Public Key and Certificate Usage

A Relying Party should only use a public key for the purposes indicated in the certificate *Key Usage* extension.  Relying Parties should not use expired or revoked encryption certificates.  If the *Extended Key Usage* extension is present and implies any limitation on the use of the certificate, those constraints should also be followed.

## 4.6 CERTIFICATE RENEWAL

Renewing a certificate consists of creating a new certificate with a new validity period and serial number while retaining all other Subscriber information in the original certificate including the public key.  Certificate renewal may be performed by any CA authorized to use the name space in the Subject DN of the certificate, potentially resulting in different key identifiers and a different CRL distribution point.

After certificate renewal, the old certificate may or may not be revoked, but shall not be further re-keyed, renewed, or modified.

### 4.6.1 Circumstances for Certificate Renewal

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

- The total key validity lifetime for that public key (including the new certificate and any previous renewals or modifications of the certificate) does not exceed the key validity lifetimes defined in Section 6.3.2
- The certificate has not reached the end of its validity period
- The certificate has not been revoked
- The name and other information in the certificate is still correct
- The identity proofing of the PKI Sponsor is current

The following table identifies identity proofing requirements for the PKI Sponsor.

**Table 4-1: Identity Proofing Requirements**

| Subscriber Type | Certificate Type | Identity Proofing Requirement |
|---|---|---|
| Name | Identity | Performance of identity proofing in accordance with Section 3.2.3.1 no more than six years prior to re-keyed certificate expiration date |
| Name | Encryption, Signature, Code Signing, Content Signing | Proof of possession of a current valid identity certificate by the PKI Sponsor |
| Role | Any | Proof of possession of a current valid identity certificate by the PKI Sponsor |
| System or Device | Any | Proof of possession of a current valid identity certificate by the PKI Sponsor |

Member CAs may also renew Subscriber certificates after the CA re-keys if all of the preceding requirements are met.

### 4.6.2 Who May Request Renewal

The PKI Sponsor, TA, or RA may request renewal of a certificate.

### 4.6.3 Processing Certificate Renewal Requests

A certificate may be renewed based on an electronically authenticated request from the PKI Sponsor using a current valid Identity certificate issued by the NSS PKI and its associated private key, subject to the following restrictions:

- Under no case shall a certificate asserting the *id-CNSS-software* policy be used for authentication for the renewal of a certificate asserting the *id-CNSS-hardware* policy
- The DN of the new certificate and, information that could be used for authorizations shall be identical to that within the identity certificate used as an authentication credential
- The expiration date of the new certificate will be no later than the next required in-person authentication date associated with the certificate used as an authentication credential
- The in-person identity proofing date associated with a new certificate will be no later than the in-person identity proofing date associated with the certificate used for authentication
- The key lifetime period will not be exceeded by the renewed certificate
- 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

The CAS or RA shall verify that the PKI Sponsor who has been electronically authenticated is the PKI Sponsor for the Subscriber identified in the certificate associated with the renewal request. The CAS or RA shall process the renewal request upon validation of the request from the PKI Sponsor.

Certificates asserting the *id-CNSS-software* OID shall be accepted only for renewal of Signature or Encryption Name Subscriber certificates asserting the *id-CNSS-software* OID. Certificates asserting the *id-CNSS-hardware* OIDs may be accepted to authenticate requests for renewal of certificates asserting the *id-CNSS-software*, *id-CNSS-hardware*, or *id-CNSS-device* OIDs.

### 4.6.4 Notification of New Certificate Issuance to Subscriber

The CAS or RA shall notify the PKI Sponsor of certificate issuance and provide instructions for retrieval of the renewed certificate.

### 4.6.5 Conduct Constituting Acceptance of a Renewed Certificate

A PKI Sponsor's request to obtain new certificates and subsequent failure to object to the certificate or its contents shall constitute acceptance of the certificate. For certificate renewals requested by an RA, RA notification to the PKI Sponsor and subsequent failure of the PKI Sponsor to object to the certificate or its contents shall constitute acceptance of the certificate.

### 4.6.6 Publication of the Renewed Certificate by the CA

See Section 2.2.

### 4.6.7 Notification of Certificate Issuance by the CA to Other Entities

The NSS PKI PMA and NSS PKI Member Governing Body shall be notified whenever a CA operating under this policy renews a CA certificate.

## 4.7 CERTIFICATE RE-KEY

Re-keying a certificate consists of creating a new certificate with a new validity period, serial number, and public key while retaining all other Subscriber information in the original certificate. Certificate re-key may be performed by any CA authorized to use the name space in the Subject DN of the certificate, potentially resulting in different key identifiers and a different CRL distribution point.

After certificate re-key, the old certificate may or may not be revoked, but shall not be further re-keyed, renewed, or modified.

### 4.7.1 Circumstances for Certificate Re-Key

A certificate may be re-keyed if all of the following are true:

- The certificate has not reached the end of its validity period
- The certificate has not been revoked
- The name and other information in the certificate is still correct
- The identity proofing of the PKI Sponsor is current (see Section 4.6.1)
- The CA or RA re-validates proof of possession of the old private key by the PKI Sponsor

### 4.7.2 Who May Request Re-Key

The PKI Sponsor, TA, or RA may request re-key of a Subscriber certificate.

### 4.7.3 Processing Certificate Re-Key Requests

A certificate may be re-keyed based on an electronically authenticated request from the PKI Sponsor using a current valid identity certificate issued by the NSS PKI and its associated private key, subject to the following restrictions:

- Under no case shall a certificate asserting the *id-CNSS-software* policy be used for authentication for the re-key of a certificate asserting the *id-CNSS-hardware* policy
- The DN of the new certificate and, information that could be used for authorizations shall be identical to that within the identity certificate used as an authentication credential
- The expiration date of the new certificate will be no later than the next required in-person authentication date associated with the certificate used as an authentication credential
- The in-person identity proofing date associated with a new certificate will be no later than the in-person identity proofing date associated with the certificate used for authentication

- 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

The CAS or RA shall process the re-key request upon validation of the request from the PKI Sponsor, ensuring that the in-person identity proofing period will not be exceeded by the re-keyed certificate.

Certificates asserting the *id-CNSS-software* OID shall be accepted only for re-key of Signature or Encryption Name Subscriber certificates asserting the *id-CNSS-software* OID. Certificates asserting the *id-CNSS-hardware* OIDs may be accepted to authenticate requests for re-key of certificates asserting the *id-CNSS-software*, *id-CNSS-hardware*, or *id-CNSS-device* OIDs.

### 4.7.4 Notification of New Certificate Issuance to Subscriber

The CAS or RA shall notify the PKI Sponsor of certificate issuance and provide instructions for retrieval of the re-keyed certificate.

### 4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

A PKI Sponsor request to obtain new certificates and subsequent failure to object to the certificate or its contents shall constitute acceptance of the certificate. For certificate re-keys requested by an RA, RA notification to the PKI Sponsor and subsequent failure of the PKI Sponsor to object to the certificate or its contents shall constitute acceptance of the certificate.

### 4.7.6 Publication of the Re-Keyed Certificate by the CA

See Section 2.2.

### 4.7.7 Notification of Certificate Issuance by the CA to Other Entities

The NSS PKI PMA and NSS PKI Member Governing Body shall be notified whenever a CA operating under this policy issues a CA certificate.

## 4.8 CERTIFICATE MODIFICATION

Modifying a certificate consists of creating a new certificate with a new serial number that differs in one or more fields from the old certificate. The new certificate may have the same or different subject public key. Certificate modification may be performed by any CA authorized to use the name space in the Subject DN of the new certificate.

After certificate modification, the old certificate may or may not be revoked, but shall not be further re-keyed, renewed, or modified.

### 4.8.1 Circumstances for Certificate Modification

A certificate may be modified if information contained in the certificate that is not used for authorization has changed. If the Subscriber DN or other information that could be used for authorization has changed, the Subscriber shall undergo the initial registration process.

If the modified certificate will have the same public key as the original certificate, the requirements for Certificate Renewal as stated in Section 4.6.1 also apply.

If the modified certificate will have a new public key, the requirements for Certificate Re-Key as stated in Section 4.7.1 also apply.

### 4.8.2 Who May Request Modification

The PKI Sponsor, TA, or RA may request modification of a Subscriber certificate.

### 4.8.3 Processing Certificate Modification Requests

A certificate may be modified based on an electronically authenticated request from the PKI Sponsor using a current valid identity certificate issued by the NSS PKI and its associated private key, subject to the following restrictions:

- Under no case shall a certificate asserting the *id-CNSS-software* policy be used for authentication for the modification of a certificate asserting the *id-CNSS-hardware* policy
- The DN of the new certificate and, information that could be used for authorizations shall be identical to that within the identity certificate used as an authentication credential
- The expiration date of the new certificate will be no later than the next required in-person authentication date associated with the certificate used as an authentication credential
- The in-person identity proofing date associated with a new certificate will be no later than the in-person identity proofing date associated with the certificate used for authentication
- 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

The CAS or RA shall process the modification request upon validation of the request from the PKI Sponsor, ensuring that the key lifetime period and the in-person identity proofing period will not be exceeded by the modified certificate.

Certificates asserting the *id-CNSS-software* OID shall be accepted only for modification of Signature or Encryption Name Subscriber certificates asserting the *id-CNSS-software* OID. Certificates asserting the *id-CNSS-hardware* OIDs may be accepted to authenticate requests for modification of certificates asserting the *id-CNSS-software, id-CNSS-hardware*, or *id-CNSS-device* OIDs.

### 4.8.4 Notification of New Certificate Issuance to Subscriber

See Section 4.6.4 for a modified certificate that has the same public key as the original certificate.

See Section 4.7.4 for a modified certificate that has a new public key.

### 4.8.5 Conduct Constituting Acceptance of a Modified Certificate

A PKI Sponsor’s request to obtain new certificates and subsequent failure to object to the certificate or its contents shall constitute acceptance of the certificate. For certificate modifications requested by an RA, RA notification to the PKI Sponsor and subsequent failure of the PKI Sponsor to object to the certificate or its contents shall constitute acceptance of the certificate.

### 4.8.6 Publication of the Modified Certificate by the CA

See Section 2.2.

### 4.8.7 Notification of Certificate Issuance by the CA to Other Entities

The NSS PKI PMA and NSS PKI Member Governing Body shall be notified whenever a CA operating under this policy issues a CA certificate.

## 4.9 CERTIFICATE REVOCATION AND SUSPENSION

The CAS or RA shall authenticate all revocation requests.

### 4.9.1 Circumstances for Revocation

A certificate shall be revoked when the binding between the subject and the subject's public key defined within a certificate is no longer considered valid. Circumstances that invalidate the binding include the following:

- Identifying information or affiliation components of any names in the certificate become invalid
- Information not included in the certificate but required for the issuance of the certificate becomes invalid (e.g., having an account on an accredited U.S. SECRET information system or network)
- Privilege attributes asserted in the certificate are no longer accurate
- The PKI Sponsor can be shown to have violated the stipulations of the PKI Sponsor agreement
- The private key is suspected of compromise
- For Name Certificates, the individual named in the certificate is no longer authorized to hold the certificate
- For Role certificates, an entity who is no longer authorized as a holder of that role may have access to the private key associated with the Role certificate
- An Intermediate or Subordinate CA is no longer meeting the requirements of this CP
- For cross certificates, the cross-certified NSS PKI is no longer meeting the requirements of this CP as specified in its MOA
- The NSS PKI PMA or NSS PKI Member Governing Body has determined that cross-certification or subordination is no longer in the best interests of the Federal Government

Whenever any of the above circumstances occur, the associated certificate shall be revoked.

A certificate shall also be revoked if the PKI Sponsor or other authorized party requests revocation of the certificate.

If control of a Sponsor cryptographic module is suspected to have been lost, this shall be immediately reported, and the certificates revoked or suspended pending investigation. If loss of control is confirmed, all associated certificates shall be revoked, and the cryptographic module shall be technically prohibited from being further keyed, and destroyed if possible.

### 4.9.2 Who Can Request a Revocation

A CA may summarily revoke certificates it has issued. A written notice and brief explanation for the revocation shall subsequently be provided to the PKI Sponsor. PKI Sponsors are authorized to request revocation of their own certificates. Other parties may request revocation of certificates by providing a reason for the revocation request to an RA.

The NSS PKI PMA and NSS PKI Member Governing Body are authorized to request revocation of CA certificates, cross certificates, or end entity certificates.

If the Root CA or an Intermediate CA determines that a Subordinate CA is not meeting the requirements of this CP, or an emergency has occurred that may affect the integrity of the NSS PKI, the Root CA or Intermediate CA is authorized to revoke the Subordinate CA certificate. Where possible, the Root CA or Intermediate CA shall first attempt to resolve the issue without revoking the certificate.

### 4.9.3 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). All revocation requests shall be verified to ensure that they have appropriate justification and are authentic to prevent malicious revocation of certificates by unauthorized parties.

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 shall so indicate. If an 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 an RA, verification of the signature is sufficient. Requests can be authenticated using the private key associated with the certificate that is being requested to be revoked.

If the revocation request can be authenticated using the certificate that is being requested to be revoked, the CA may validate the request and revoke the certificate. All other requests shall be authenticated by an RA. In emergency cases where the requestor is not an authorized party, the RA shall take measures to verify the authority of the requestor and the need for revocation. In general, the RA may, at his or her discretion, take reasonable measures to verify the need for revocation. If the revocation request appears to be valid, the RA shall approve the revocation of the certificate.

The CA shall revoke the certificate by placing its serial number and other identifying information on a CRL, in addition to any other revocation mechanisms used. Revoked certificates shall be included on at least one CRL, and shall be included on all new publications of the CRL until the certificates expire. Revocation takes effect upon initial publication of the CRL containing the revocation information.

For hardware certificates, revocation is optional only if all of the following conditions are met:

- The revocation request was not for key compromise
- The hardware token does not permit the user to export the private key
- The PKI Sponsor surrendered the token to an RA Officer or TA
- The token was zeroized or destroyed by the RA Officer or TA upon surrender
- The token was protected from malicious use between surrender and zeroization and destruction
- An audit record of token surrender, protection, and zeroization is maintained

In all other cases, revocation is mandatory. If the token is not recovered from the Subscriber or protected from malicious use prior to zeroization, then all certificates associated with the token shall be revoked for the reason of key compromise. If it is determined 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 also be revoked.

The revoking authority shall immediately notify the NSS PKI PMA and any Intermediate, Subordinate, or cross-certified ANMAs if the signing certificate for any Intermediate or Subordinate CA is revoked for any reason.

If the revocation is a result of the subscriber or sponsor leaving the organization, the ANMA shall require the surrender of the token from the subscriber or sponsor.

### 4.9.4 Revocation Request Grace Period

There is no grace period for revocation under this CP.

### 4.9.5 Time within Which CA Must Process the Revocation Request

A CA shall revoke certificates as quickly as practical upon receipt of a proper revocation request. Revocation requests shall be processed before the next CRL is published (See Table 4-2), excepting those requests for reasons other than compromise, which are validated within two hours of the next CRL issuance. Such revocation requests shall be processed before the following CRL is published. A request is considered received when a CAS or RA first accesses a valid request.

### 4.9.6 Revocation Checking Requirements for Relying Parties

Use of revoked certificates could have damaging or catastrophic consequences in certain applications. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party. Revocation data should be obtained from an authoritative source, such as a CRL or an authoritative CSS as defined in Section 1.3.2.4. CAS and RA components shall only use CRLs or authoritative CSSs.

If it is temporarily infeasible to obtain revocation information from an authoritative source, then the Relying Party should 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.

### 4.9.7 CRL Issuance Frequency

CRLs shall be 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. CAs shall always post an early update to an applicable Revocation List (CRL) in the event of a revocation due to key compromise. CAs shall ensure that superseded CRLs are removed from the repository upon posting of the latest CRL.

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

**Table 4-2: CRL Issuance Requirements**

| CA Type | Normal CRL Issuance | Issuance as a Result of Key Compromise | Next Update Latency |
|---|---|---|---|
| **Root CA** | At least once every 31 days | Within 18 hours of notification | Minimum: issuance frequency + 1 day<br>Maximum: issuance frequency + 7 days |
| **Intermediate CA (Operated Off-line)** | At least once every 31 days | Within 18 hours of notification | Minimum: issuance frequency + 1 day<br>Maximum: issuance frequency + 7 days |
| **Intermediate CA (Operated On-line)** | At least once every 24 hours | Within 18 hours of notification | Minimum: issuance frequency + 4 hours<br>Maximum: issuance frequency + 6 days |
| **Subordinate CA** | At least once every 24 hours | Within 6 hours of notification | Minimum: issuance frequency + 4 hours<br>Maximum: issuance frequency + 6 days |

NSS PKI CRLs shall be published upon generation, but within no more than four hours after generation. Each CRL shall be published no later than the time specified in the *nextUpdate* field of the previously issued CRL for the same scope.

### 4.9.8 Maximum Latency for CRLs

In order to ensure that Relying Parties may obtain a current, valid CRL, the time indicated in the *nextUpdate* field of the CRL shall be past the time indicated in the *thisUpdate* field by a minimum of the latency indicated; and not past the time indicated in the *thisUpdate* by more than the maximum of the latency indicated in Section 4.9.7.

### 4.9.9 On-line Revocation/Status Checking Availability

A CA may use a CSS to support on-line revocation status checking. See Section 4.10 for CSS requirements.

### 4.9.10 On-line Revocation Checking Requirements

If supported, Relying Parties may use a CSS to determine certificate validity. Relying Parties using a CSS supported by the NSS PKI need not obtain or process CRLs. See Section 4.10 for CSS requirements.

### 4.9.11 Other Forms of Revocation Advertisements Available

A CA may use a CSS to support other methods to publicize the status of certificates. See Section 4.10 for CSS Requirements.

### 4.9.12 Special Requirements Related to Key Compromise

See Sections 4.9.7 and 5.7.1 for incident and compromise handling and Section 5.7.3 for entity private key compromise procedures. See Section 4.9.3 for revocation procedures.

### 4.9.13 Certificate Suspension and Restoration

CAs may support certificate suspension and restoration.

#### *4.9.13.1 Circumstances for Suspension*

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

- The PKI Sponsor for the certificate has misplaced the token containing the private key associated with the certificate, but believes that the token is in a protected location
- The PKI Sponsor is known or believed to have the token containing the private key associated with the certificate, and fails to appear at an expected duty location

#### *4.9.13.2 Who Can Request Suspension*

PKI Sponsors are authorized to request suspension of their own certificates. Other parties, including the manager, supervisor, or superior officer, may request suspension of certificates by providing a reason for the suspension request to an RA or TA.

#### *4.9.13.3 Procedure for Suspension Request*

Any format that is used to request a suspension shall identify the certificate to be suspended, explain the reason for suspension, include an estimated time for the resolution of the suspension, and allow the request to be authenticated (e.g., digitally or manually signed). Prior to approving a certificate suspension, the RA shall verify the suspension request, to include authenticating the identity of the requestor via means commensurate with the requirements of the data to be protected by the certificates being suspended, and verifying the requestor's authority to request suspension and the validity of the reason for the suspension request.

Once approved by the RA, the CA shall suspend the certificate and place its serial number and other identifying information on a CRL, in addition to any other suspension or revocation advertisement mechanisms used.

#### *4.9.13.4 Limits on Suspension Period*

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

#### *4.9.13.5 Circumstances for Restoration*

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

#### *4.9.13.6 Who Can Request Restoration*

The party that requested suspension of the certificate is authorized to request restoration by providing a reason for the restoration to an RA through an authenticated mechanism.

PKI Sponsors may request restoration of their own certificates. Other parties may request restoration of certificates by providing a reason for the restoration to an RA or TA.

#### *4.9.13.7 Procedure for Restoration Request*

The request for a restoration shall identify the certificate to be restored, provide the reason for restoration, and shall be digitally or manually signed. Prior to approving a certificate restoration, the RA shall validate the restoration request to include:

- Ensuring the request has appropriate justification
- Authenticating the identity of the requestor
- Verifying the requestor’s authority to request restoration
- Verifying the integrity of the request at a level commensurate with the certificate being restored

If a PKI Sponsor requests restoration of their own certificate, the RA shall validate the identity of the PKI Sponsor, and the validity of the reason for restoration, prior to restoration of the certificate.

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

The CA shall restore the certificate by removing its serial number and other identifying information from the next CRL and all future CRLs until the certificate expires or is revoked. The CA shall also restore the certificate to a valid state in any other revocation or suspension mechanisms used.

For Name Certificates, the manager, supervisor, or superior officer shall determine the circumstances for the suspension and if restoration is warranted in accordance with organizational practices relative to the circumstances for the suspension. If the circumstances warrant, the manager, supervisor, or superior officer shall inform, in an authenticated manner commensurate with the information that the suspended certificate protects, the RA to change the status of the certificate from suspended to revoked.

Once a certificate has been revoked, it shall not be restored.

## 4.10 CERTIFICATE STATUS SERVICES

CSSs are not a required component of the NSS PKI. If supported as part of the NSS PKI (See Section 1.3.2.4), the CSS is considered an integral part of the CAS and, except where expressly noted, all requirements imposed on CASs apply.

### 4.10.1 Operational Characteristics

A CSS shall meet the following requirements:

- The CSS shall be operated in compliance with this CP and any applicable Internet standards
- Information exchanged between the CA and the CSS shall be authenticated and protected from modification using mechanisms commensurate with the requirements of the data to be protected by the certificates being issued
- Accurate and up-to-date information from the associated CA shall be used to provide the revocation status
- Revocation status responses shall provide authentication and integrity services commensurate with the requirements of the data to be protected by the certificates being issued, to include the status of the certificate and the time the status indication was generated
- Latency of certificate status information shall meet or exceed the requirements for CRL issuance stated in Section 4.9.7
- Each certificate in the certificate chain used to validate the certificate whose status is being requested is checked for revocation, such that the Relying Party need not check more than one authority to validate a Subscriber certificate

### 4.10.2 Service Availability

No stipulation.

### 4.10.3 Optional Features

No stipulation.

## 4.11 END OF SUBSCRIPTION

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

## 4.12 KEY ESCROW AND RECOVERY

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

### 4.12.1 Key Escrow

#### *4.12.1.1 Circumstances for Key Escrow*

Private keys associated with encryption certificates shall be escrowed prior to certificate issuance. Private keys associated with Identity, Signature, Code Signing, or Content Signing certificates shall never be escrowed.

#### *4.12.1.2 Escrowing Keys*

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

Escrowed keys shall be maintained within the KES for a minimum of one year after the expiration of the certificate associated with the key. If the certificate associated with the key is renewed or modified without changing the key, the escrowed key shall be maintained within the KES for a minimum of one year after the expiration date of the renewed or modified certificate associated with the key. Escrowed keys shall be archived as described in Section 5.5. KES security audit requirements related to the CAS and RA are specified in Section 5.4.

#### *4.12.1.3 Notification of Key Escrow to Subscriber*

As part of the key escrow process, all subscribers shall be notified that the private keys associated with their encryption certificates will be escrowed.

### 4.12.2 Key Recovery

The NSS PKI supports the mechanism for obtaining a copy of an escrowed key where access to that key is a necessary condition for access to data. The NSS PKI does not provide a data recovery service, nor is this CP intended to change the authority of any individual or organization to access data.

Recovery of private keys associated with expired encryption certificates may be performed as part of the re-key process to ensure that earlier encryption private keys are contained on re-keyed tokens. Recovered keys associated with certificates that assert the *id-CNSS-hardware* OID shall only be recovered to another token that meets the requirements specified in Section 6.2.1 for certificates that assert the *id-CNSS-hardware* OID.

During delivery, escrowed keys shall be protected against disclosure to any party except the requestor and the trusted roles responsible for the recovery.

Key recovery archive requirements are as described in Section 5.5. Key recovery security audit requirements are specified in Section 5.4.

#### *4.12.2.1 Circumstances for Key Recovery*

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

- The original copy of the escrowed key has been lost or damaged and the Subscriber cannot access data encrypted with the corresponding public key
- The certificate is to be re-keyed and the earlier issued private keys are recovered to be included on the token containing the re-keyed certificate
- An authorized third party (other than the PKI Sponsor) requires access to data encrypted with the corresponding public key

#### *4.12.2.2 Who May Request Key Recovery*

PKI Sponsors may request recovery of their own escrowed keys. RAs may request initiation of the recovery of escrowed keys as part of the re-key process. Key recovery may also be requested by the following third parties:

- PKI Sponsor's manager, supervisor, or superior officers
- Law enforcement or counterintelligence agents
- Agents of U.S. Federal Courts
- Any person or organization authorized by the NSS PKI PMA or ANMA via an authenticated communication

#### *4.12.2.3 Processing Key Recovery Requests*

PKI Sponsors may electronically submit requests on their own behalf directly to an RA. Such requests shall be signed by a private key associated with a valid NSS PKI issued Identity or Signature certificate asserting the same policy as that of the certificate associated with the escrowed key.

PKI Sponsors may use automated means to request their escrowed keys from the KES if they possess a valid NSS PKI issued Identity certificate asserting the same policy OID as that of the certificate associated with the escrowed key. The KES shall only provide escrowed keys to current PKI Sponsors via an automated means after performing all of the following:

- Verifying that the authenticated identity of the requestor is the same as the PKI Sponsor associated with the escrowed keys being requested
- Attempting to notify the PKI Sponsor of the attempts (successful or unsuccessful) to recover the escrowed keys that are made by entities claiming to be the PKI Sponsor. If the KES does not have information (e.g., an e-mail address) necessary to attempt to notify the PKI Sponsor of a key recovery request, then the KES shall not provide the PKI Sponsor with the requested key material using the automated recovery process
- Ensuring that the escrowed keys are being sent only to the authenticated PKI Sponsor associated with the escrowed keys
- Ensuring that the recovered keys are encrypted during transmission in accordance with Section 6.2.6 and that activation data used to protect access to the recovered keys is in accordance with Section 6.4.1.

PKI Sponsors may submit a request, signed by hand, to either an RA Officer or TA. The RA Officer or TA shall validate the identity of the requestor, and RA Officer shall determine the authority of the requestor to recover the escrowed key. TAs shall forward the request via a digitally signed mechanism to an RA Officer. The RA Officer shall authenticate the information in the request. This may be by separate channel means.

Third party requestors shall submit requests to either an RA Officer or a TA. Paper requests shall be hand-signed; electronic requests shall be digitally signed by a private key associated with a valid NSS PKI issued identity or signature certificate. The RA Officer or TA shall validate the identity of the requestor and the RA Officer shall determine the authority of the requestor to recover the escrowed key in consultation with organization management and/or legal counsel, as appropriate. TAs shall forward information via a digitally signed mechanism to an

RA Officer. Third party key recovery operations shall be performed under the control of two individuals holding trusted roles, at least one of whom shall be an RA Officer.

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

The RA Officer shall authenticate to the KES using a mechanism commensurate with the cryptographic strength of the strongest key stored in the KES. Once an RA Officer has received and validated a key recovery request, the RA shall initiate the key recovery.

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

#### *4.12.2.4 Notification of Key Recovery to Subscriber*

PKI Sponsors shall be notified of all attempts to recover escrowed keys based on a request using a PKI Sponsor’s private key.

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

#### *4.12.2.5 Notification of Key Recovery by the CA to Other Entities*

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

# 5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

## 5.1 PHYSICAL CONTROLS

All CAS and RA equipment, including cryptographic modules, shall be protected from theft, loss, and unauthorized access at all times. Unauthorized use of CAS and RA equipment is prohibited. CAS and RA equipment shall be dedicated to performing CAS and RA functions.

### 5.1.1 Site Location and Construction

The location and construction of facilities housing all NSS PKI CAS and RA equipment and operations shall be located in facilities and/or office areas approved by agency security officials for processing of classified information of the highest classification that will be asserted in or protected by use of a certificate issued by or through that equipment or SECRET, whichever is higher. PKI, while not COMSEC material, should be appropriately protected.

(See *CNSS 4005, Safeguarding COMSEC Facilities and Material* [CNSS 4005] for a description of physical security requirements. Local requirements are also in effect.)

### 5.1.2 Physical Access

Physical access to CAS equipment shall be limited to CAS Operations Staff and Security Auditors. The security mechanisms shall be commensurate with the level of threat in the equipment environment.

At a minimum, physical access controls for CAS equipment and all copies of the CA cryptographic module shall meet the following requirements:

- Ensure that no unauthorized access to the hardware is permitted
- Ensure that all removable media and paper containing sensitive plain-text information is stored in secure containers
- Be manually or electronically monitored for unauthorized intrusion at all times
- Ensure an access log is maintained and inspected periodically
- Require two-person physical access control. At least one individual shall be a member of the CAS Operations Staff. Technical or mechanical mechanisms (e.g., dual locks) shall be used to enforce the two-person physical access control.

When not in use, removable CAS cryptographic modules, removable media, and any activation information used to access or enable CAS cryptographic modules or CAS equipment, or paper containing sensitive plain-text information 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. Access to the contents of the locked containers shall be restricted to individuals holding CAS trusted roles as defined in Section 5.2, utilizing two-person access controls, and two-person integrity while the container is unlocked.

CAS cryptographic modules held within the work area for intermittent use throughout the day may be kept under one lock in an area requiring the presence of more than one person at all times. Knowledge of the combination or access to the key used to secure the lock shall be restricted to the supervisor on duty. When in active use, the cryptographic module shall be locked into the system (rack, reader, server, etc.) using a physical lock to prevent unauthorized removal.

Any activation information used to access or enable the cryptographic modules or CAS equipment shall be stored separately from the associated modules and equipment. Such information shall either be memorized or recorded and stored in a manner commensurate with the security afforded the associated cryptographic module or equipment.

A security check of the facility housing CAS equipment shall occur prior to leaving the facility unattended. The check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when “open”, and secured when “closed”)
- Any security containers are properly secured
- Physical security systems (e.g., door locks, vent covers) are functioning properly
- The area is secured against unauthorized access

If unattended for periods greater than 24 hours, a facility housing CAS equipment shall 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. 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.

RA equipment shall be protected from unauthorized access while the cryptographic module is installed and activated. RAs 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.

At a minimum, the cryptographic module shall be maintained in the positive control of the PKI Sponsor or authorized user. Any loss of control shall be reported immediately.

### 5.1.3 Power and Air Conditioning

A facility that houses CAS or RA equipment shall be supplied with power and air conditioning sufficient to provide reliable operation.

CAS equipment shall have backup power and air conditioning capability sufficient to allow for the automatic and proper lockout of input, completion of any pending actions, and recording of the state of the equipment before lack of power or air conditioning causes a shutdown.

### 5.1.4 Water Exposures

CAS and RA equipment shall be installed such that it is not in danger of exposure to water, and ensure installation of moisture detectors in areas susceptible to flooding. If the CAS equipment location has sprinklers for fire control, the CAS 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

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

A description of the CAS's approach for recovery from a fire disaster shall be included in the Disaster Recovery Plan (see Section 5.7.4).

### 5.1.6 Media Storage

Media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic) and unauthorized physical access. Media not required for daily operation or not required by policy to remain with the CAS or RA that contains security audit, archive, or backup information shall be stored in a location separate from the CAS or RA equipment.

Media containing private key material, other than cryptographic modules containing Subscriber private keys, shall be handled, packaged, and stored in a manner compliant with the requirements for the classification level of the information it protects or provides access. Cryptographic modules containing Subscriber private keys shall be consistent with Section 5.1.2. Storage protection of CAS and RA private key material shall be consistent with stipulations in Section 5.1.2 and Section 6.2.

### 5.1.7 Waste Disposal

CAS and RA Operations Staff shall remove and destroy normal office waste in accordance with local policy. Media used to collect or transmit information discussed in Section 9.4 shall be destroyed, such that the information is unrecoverable, prior to disposal. Classified media and paper shall be destroyed in accordance with the applicable policy for destruction of such material.

Destruction of media containing private key material shall comply with stipulations in Section 6.2.10.

### 5.1.8 Off-site Backup

System backups sufficient to recover from system failure shall be made on a periodic schedule. Backups shall be performed and stored off-site not less than once per week or when a CAS is operational, whichever is less frequent. At least one backup copy shall be stored at an offsite location separate from the CAS 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 CAS system.

The data backup media shall be stored in a facility approved for storage of information of the same value or classification of the information that will be protected by the certificates and associated private keys issued or managed using the equipment with a minimum requirement of transferring, handling, packaging, and storage of the information in a manner compliant with requirements for SECRET material identified in Section 5.1.2.

## 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 shall be held accountable to perform designated actions correctly or the integrity of the CAS is weakened. The functions performed in these roles form the basis of trust in the entire NSS 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.

The CAS 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.

The only trusted roles defined by this policy are the CAS Operations Staff, the RA Operations Staff (including RA Officers), TAs, and Security Auditors. Other trusted roles may be defined in other documents, which describe or impose requirements on the CAS operation.

#### *5.2.1.1 CAS Operations Staff*

CAS Operations Staff is defined in Section 1.3.2 as the individuals holding trusted roles that operate and manage CAS components. CAS Operations Staff is responsible for the following:

- Installation, configuration, and maintenance of the CAS
- Establishing and maintaining CAS operating system and application accounts
- Configuring certificate profiles or templates and audit parameters
- Generating and backing up CAS keys
- Approving infrastructure certificates issued to support the operations of the CAS (except for CA signing certificates which must be approved by the PMA or issuing ANMA)
- Approving revocation of certificates issued to CASs or to support the operations of the CAS
- Routine operation of the CAS equipment such as system backup and recovery or changing recording media
- Approving certificates issued to RAs
- Authorizing RAs
- Approving revocation of certificates issued to RAs
- Posting Certificates and CRLs
- Ensuring certificate generation and revocation occur according to the stipulations of this policy
- Controlling and managing CAS cryptographic modules

- Providing Certificate revocation and suspension status information as part of a CSS (if implemented)
- Providing escrow and recovery of subscriber private keys associated with encryption certificates
- Administrative functions such as compromise reporting and maintaining internal databases

#### *5.2.1.2 RA Operations Staff*

RA Operations Staff is defined in Section 1.3.3 as the individuals holding trusted roles that operate and manage RA components. RA Operations Staff is responsible for the following:

- Installation, configuration, and maintenance of the RA
- Establishing and maintaining RA operating system and application accounts
- Routine operation of the RA equipment such as system backup and recovery or changing recording media

RA Officers are considered part of the RA Operations Staff and may perform some or all of the above functions. In addition, RA Officers are specifically responsible for the following:

- Registering new Subscriber and requesting the issuance of certificates
- Verifying the identity of PKI Sponsors
- Verifying the accuracy of information included in certificates
- Approving and executing the issuance of certificates
- Requesting, approving, and executing the suspension, restoration, and revocation of certificates
- Verifying the identity and authorization of entities requesting recovery of escrowed key material
- Authorizing and facilitating the recovery of escrowed key material
- Recovering escrowed key material if assigned that responsibility by the ANMA
- Distributing recovered copies of escrowed keys to requestors, with protection as described in Section 6.2.6 and Section 6.4.1

#### *5.2.1.3 Trusted Agent*

A Trusted Agent is defined in Section 1.3.4 as an individual holding a trusted role that assists in performing RA Officer responsibilities. However, a TA does not have privileged access to any CAS components to authorize certificate issuance, certificate revocation, or key recovery. A TA may be responsible for the following:

- Verifying the identity of PKI Sponsors
- Verifying the accuracy of information to be included in certificates
- Verifying the identity and authorization of entities requesting certificate revocation, suspension, or restoration
- Verifying the identity and authorization of entities requesting recovery of escrowed key material

#### *5.2.1.4 Security Auditor*

Security Auditors are responsible for auditing CASs and RAs as defined in Section 5.4. Security Auditors are responsible for the following:

- Reviewing, maintaining, and archiving audit logs
- Performing or overseeing internal audits to ensure that CASs are operating in accordance with the associated CPSs
- Performing or overseeing internal audits to ensure that RAs are operating in accordance with the associated CPS or RPS

### 5.2.2 Number of Persons Required per Task

Where multiparty control is required, all participants shall hold a trusted role. Multiparty control shall not be achieved using personnel that serve in a Security Auditor role with the exception of audit functions, which require the participation of a Security Auditor. The following tasks shall require two or more persons:

- Generation, activation, and backup of CAS keys
- Performance of CAS administration or maintenance tasks
- Archiving or deleting CAS audit logs (Note, at least one of the participants shall serve in a Security Auditor role)
- Physical access to CAS equipment
- Access to any copy of the CAS cryptographic module
- Processing of third party key recovery requests

Requirements for multi-person control of CAS private keys are described in Section 6.2.2.

### 5.2.3 Identification and Authentication for Each Role

Individuals holding trusted roles shall identify and authenticate themselves before being permitted to perform any actions set forth above for that role or identity. CAS and RA equipment shall require, at a minimum, strong (e.g., cryptographically-based) authenticated access control for remote access using NSS PKI issued credentials. CAS Operations Staff and RA Officers shall authenticate using a credential that is distinct from any credential they use to perform non-trusted role functions. CAS and RA equipment shall require, at a minimum, authenticated access control (e.g., strong passwords) for local access.

Individuals holding trusted roles shall be appointed and approved to hold the trusted role by an appropriate approving authority. The approval shall be recorded in a secure and auditable fashion. Individuals holding trusted roles shall accept the responsibilities of the trusted role, and this acceptance shall be recorded in a secure and auditable fashion.

### 5.2.4 Roles Requiring Separation of Duties

Individuals serving as Security Auditors shall not perform or hold any other trusted role.

An individual that holds any CAS Operations Staff role shall not be an RA Officer.

Under no circumstances shall any holder of a trusted role perform its own compliance audit. Only an individual serving in a Security Auditor role may perform internal auditing functions, with the exception of those security audit functions (e.g., configuring, archiving, deleting) that require multi-person control (see Section 5.2.2).

An individual that performs any trusted role shall only have one identity when accessing CAS equipment.

## 5.3 PERSONNEL CONTROLS

### 5.3.1 Qualifications, Experience, and Clearance Requirements

Individuals appointed to any trusted role shall meet the following:

- Be employees of a CNSS member agency or be a contractor/vendor employee contracted to a CNSS member agency
- Be within the administrative control of an identified administrator who is a CNSS member agency employee or a civilian contractor/vendor employee of equivalent or greater responsibility and compensation
- Have not been denied a security clearance or had a security clearance revoked
- Be appointed in writing
- Hold a minimum clearance of a final U.S. SECRET
- Be a U.S. citizen
- Have successfully completed an appropriate training program
- Have demonstrated the ability to perform their duties
- Have no other duties that would interfere or conflict with their responsibilities as defined in Section 5.2.1
- Have not been previously relieved of trusted role duties for reasons of negligence or non-performance of duties
- Have not been convicted of a felony offense

### 5.3.2 Background Check Procedures

All individuals appointed to any trusted role shall hold a U.S. SECRET security clearance. In addition, CAS Operations Staff and Security Auditors shall have favorably completed a Single Scope Background Investigation (SSBI) covering at least the past 10 years or to age 18, whichever is less. Background checks shall be performed solely to determine the suitability of the person to fill a NSS PKI trusted role, and shall not be released except as required by law.

### 5.3.3 Training Requirements

Individuals appointed to any trusted role shall be appropriately trained. The table below indicates topics that shall be included in the training.

**Table 5-1: Training Topics**

| Topic | CA Operations Staff | RA Operations Staff | Security Auditor | TA |
|---|---|---|---|---|
| Stipulations of this policy and local guidance | X | X | X | X |
| PKI duties they are expected to perform | X | X | X | X |
| Specific PKI operational procedures | X | X | | |
| CAS operational and security principles, mechanisms and procedures | X | | X<br>(for CA) | |
| PKI software versions in use on the CAS | X | | | |
| RA operational and security principles, mechanisms, and procedures | | X | X<br>(for RA) | |
| PKI software versions in use on the RA | | X | | |
| Disaster recovery and business continuity procedures | X | X | | |

A training plan shall be established by each CAS, and training completed by personnel shall be documented.

### 5.3.4 Retraining Frequency and Requirements

All individuals holding trusted roles except TAs shall be made aware of changes in the CAS or RA operation. Any significant change to the CAS or RA operation shall have a training awareness plan, and the execution of such plan shall be documented. Examples of such changes are CAS or RA software or hardware upgrade, changes in automated security systems, and relocation of CAS or RA equipment.

### 5.3.5 Job Rotation Frequency and Sequence

This policy makes no stipulation regarding frequency or sequence of job rotation. However, a CAS shall provide for continuity and integrity of the NSS PKI service.

### 5.3.6 Sanctions for Unauthorized Actions

The PMA shall recommend the appropriate administrative and disciplinary actions be taken against personnel who have performed actions involving the Root CA that violate this policy, the applicable CPS, or other published procedures.

Likewise, the ANMA shall take or recommend the appropriate administrative and disciplinary actions against personnel who have performed actions involving a CAS or RA that violate this policy, the applicable CPS, or other published procedures.

The ANMA shall report suspected security violations or compromises to the appropriate security officials.

### 5.3.7 Independent Contractor Requirements

Contractor personnel filling trusted roles shall be subject to all requirements stipulated in this CP.

Vendors who provide services shall establish procedures to ensure that any subcontractors perform in accordance this CP and the applicable CPS.

### 5.3.8 Documentation Supplied to Personnel

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

## 5.4 AUDIT LOGGING REQUIREMENTS

Audit log files shall be generated for all events related to the security of the CAS or RA. Where possible, security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. Physical logbooks shall implement controls to allow for the detection of the removal of pages or deletion of entries. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with Section 5.5.2.

### 5.4.1 Types of Events Recorded

Security auditing capabilities of the CAS and RA system and applications shall be enabled during installation. At a minimum, each audit record shall include the following (recorded either automatically or manually for each auditable event):

- The type of event
- The date and time the event occurred
- For signing, revocation, escrow, or recovery processes, a success or failure indicator
- The identity of the entity or operator that caused the event
- For messages from RAs or any source requesting an action by the CAS, the message date and time, source, destination and contents

At a minimum, the events identified in the following table shall be recorded by each system that performs the action:

**Table 5-2: Auditable Events**

| Event Type | Event |
|---|---|
| Security Audit | • Any changes to the Audit parameters, e.g., audit frequency, type of event audited<br>• Any attempt to delete or modify the Audit logs |

| Event Type | Event |
|---|---|
| Identification and Authentication | - Successful and unsuccessful attempts to assume a role<br>- The value of maximum authentication attempts is changed<br>- The maximum number of unsuccessful authentication attempts occurs during a user login<br>- An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts<br>- An Administrator changes the type of authenticator, e.g., from password to biometrics |
| Local Data Entry | - Any security-relevant data that is entered in the system (e.g., account management, directory access, policy or privilege change) |
| Remote Data Entry | - Any security-relevant messages that are received by the system |
| Data Export and Output | - Any successful and unsuccessful requests for private, sensitive, classified, or security-relevant information |
| Key Generation | - Whenever the CAS generates a key (Not mandatory for single session or one-time use symmetric keys) |
| Private Key Load and Storage | - The loading of Component private keys<br>- Any access to certificate subject private keys retained within the CAS for key recovery purposes |
| Trusted Public Key Entry, Deletion, and Storage | - Any changes to the trusted public keys, including additions and deletions |
| Private Key Export | - The export of private keys (keys used for a single session or message are excluded) |
| Certificate Registration | - Any certificate requests |
| Certificate Status | - Any certificate revocation, modification, suspension, re-key, or renewal requests |
| Certificate Status Change Approval | - The approval or rejection of a certificate status change request |
| CAS or RA Configuration | - Any security-relevant changes to the configuration of the CAS or RA<br>- Configuration changes to the CAS or RA involving hardware, software, operating system, patches, or security profiles. |
| Account Administration | - Roles and users are added or deleted<br>- The access control privileges of a user account or a role are modified |
| Certificate Profile Management | - All changes to the certificate profile |
| Revocation Profile Management | - All changes to the revocation profile |
| CRL Profile Management | - All changes to the CRL profile |
| Personnel Controls | - Appointment of an individual to a trusted role<br>- Designation of personnel for multiparty control<br>- Training of individuals appointed to the RA role |
| Miscellaneous | - Installation of CAS and RA operating systems and applications<br>- Physical access to, loading, zeroizing, transferring keys to or from, backing-up, acquiring, or destruction of cryptographic modules<br>- Installing hardware cryptographic modules<br>- Removing hardware cryptographic modules<br>- Receipt, servicing (e.g., keying or other cryptologic manipulations), and shipping |

| Event Type | Event |
|---|---|
| | hardware cryptographic modules<br>• System startup<br>• Logon attempts to CAS or RA applications<br>• Receipt of hardware / software<br>• Attempts to set passwords<br>• Attempts to modify passwords<br>• Backing up CAS or RA internal databases<br>• Restoring CAS or RA internal databases<br>• File manipulation (e.g., creation, renaming, moving)<br>• Posting of any material to a repository<br>• Access to CAS or RA internal databases<br>• All certificate compromise notification requests<br>• Re-key of the any component private keys to include the CAS<br>• A message from any source received by any CAS requesting an action related to the operational state of the CAS<br>• Any requests and actions taken in response to messages requesting CAS actions not covered elsewhere<br>• Installation, access, and modification (to include changes in configuration files, security profiles, and administrator privileges) of CAS and RA system<br>• Any use of the CA signing key<br>• Any use of the RA signature key<br>• Messages received from any source requesting RA actions, (certificate requests, compromise notification, key recovery requests, key recovery approval)<br>• Any actions taken in response to requests for RA actions |
| Physical Access and Site Security | • Personnel access to room housing CAS<br>• Physical access to the CAS<br>• Known or suspected violations of physical security<br>• Any known or suspected violations of physical security, suspected or known attempts to attack the RA equipment via network attacks, equipment failures, power outages, network failures, or violations of this certificate policy |
| Anomalies | • Software error conditions<br>• Software check integrity failures<br>• Receipt of improper messages<br>• Misrouted messages<br>• Network attacks (suspected or confirmed)<br>• Equipment failure<br>• Electrical power outages<br>• Uninterruptible power supply (UPS) failure<br>• Obvious and significant network service or access failures<br>• Violations of certificate policy<br>• Violations of certification practice statement<br>• Resetting operating system clock<br>• Network failures |
| Key Escrow and Recovery | • Server installation, access, and modification (to include changes in configuration files, security profiles, administrator privileges)<br>• Key escrow database application access (e.g., logon/logoff)<br>• Messages received from any source requesting key escrow database actions, (e.g., escrowed key retrieval requests) |

| Event Type | Event |
|---|---|
| | • Messages sent to any destination authorizing key recovery actions, (e.g., first party escrowed key retrieval authorizations, second party key recovery approvals)<br>• Actions taken in response to requests for key escrow database actions<br>• Physical access to, loading, zeroizing, transferring keys to or from, backing-up, acquiring or destroying key escrow database cryptographic modules<br>• Receipt of keys for escrow and posting of these keys to the key escrow database<br>• Retrieval, packaging (e.g., keying or other cryptologic manipulations), securing, and shipping copies of escrowed keys;<br>• Transfer of escrowed keys to requestors<br>• Any security-relevant actions performed in support of delivery of escrowed keys<br>• Requestor identity and authorization verification (including copies of authorizations; e.g., court orders) supporting key recovery requests |

### 5.4.2 Frequency of Processing Log

Audit logs shall be reviewed by a Security Auditor at least once every month (12 per year). A statistically significant portion (at least 33 percent) of the security audit data generated since the last review shall be examined.

### 5.4.3 Retention Period of Audit Log

The information generated on the CAS or RA equipment shall be kept on the CAS or RA equipment until the information is moved to an appropriate archive facility. Audit data shall be reviewed prior to deletion from the operational system. Deletion of the security audit data from the CAS or RA equipment shall be performed by a Security Auditor. Security audit data shall be retained on-site for at least two months, then off-site as archive records in accordance with Section 5.5.2.

### 5.4.4 Protection of Audit Log

The security audit data shall not be open for reading or modification by any human, or by any automated process other than the Security Auditor and processes that perform audit functions. CAS and RA system configuration and procedures shall be implemented together to ensure that only authorized people can read, archive, or delete security audit data. The Security Auditor need not have "Modify" access to perform audit data archive, but procedures shall be implemented to protect archived data from deletion or destruction prior to the end of the security audit data retention period.

The CAS or RA shall implement procedures to ensure that the security audit data is transferred prior to overwriting or overflow of automated security audit log files. Security audit data shall be moved to a safe, secure storage location separate from the CAS or RA equipment.

Technical and/or procedural controls shall be implemented so that Security Auditors are the only individuals that have the capability to start, stop, view, backup, modify, delete, or otherwise manage audit logs.

### 5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries shall be backed up at least monthly.  A copy of the audit log shall be sent off-site on a monthly basis.

### 5.4.6 Audit Collection System (Internal Vs. External)

The security audit log collection system may or may not be external to the CAS or RA system.  The security audit process shall run independently and shall not be under the control of the CAS or RA Operations Staffs in any way.  Audit processes shall be invoked at system startup.  Only the application audit function may cease at application shutdown; the system audit function shall continue to operate until system shutdown.  Audit collection systems shall be configured such that security audit data is protected against loss (e.g., overwriting or overflow of automated log files).  Should it become apparent that an automated security audit system has failed; the CAS or RA shall cease all operation except for revocation and suspension processing until the security audit capability can be restored.

### 5.4.7 Notification to Event-Causing Subject

There is no requirement to notify a subject that an event was audited.  Real-time alerts are neither required nor prohibited.

### 5.4.8 Audit Log Assessments

The Security Auditor shall verify that the audit logs have not been tampered with, and then review the logs 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.  All significant events shall be explained in an audit log summary.  Actions taken as a result of these reviews shall be documented.

CAS and RA Operations Staff shall be watchful for attempts to violate the integrity of the CAS or RA, including the equipment, physical location, and personnel.

## 5.5 RECORDS ARCHIVAL

### 5.5.1 Types of Records Archived

Archive records shall be sufficiently detailed to establish the validity of a signature and determine the proper operation of the CAS or RA.  At a minimum, the following data shall be archived:

- Accreditation (if applicable) and any modifications, updates, etc
- This CP and any modifications, updates, etc
- Applicable CPSs and RPSs
- Any modifications or updates to CPSs and RPSs
- Contractual obligations and any modifications, updates, etc.
- Agreements concerning operations of the CAS or RA

- Any modifications or updates to agreements concerning operations of the CAS or RA
- All certificates issued and/or published
- Record of re-key
- Escrowed private keys associated with encryption certificates
- Security audit data as defined in Section 5.4.1, to include but not limited to:
    - Any changes to audit parameters and any attempt to modify or delete audit logs
    - System and equipment configuration
    - Modifications and updates to system or configuration
    - Certificate requests
    - CAS key generation
    - Changes to trusted public keys
    - Approval or rejection of status change request
    - Revocation requests
    - Destruction of cryptographic modules
- Appointment of individual to a trusted role
- Destruction of cryptographic modules
- Certificate compromise notifications
- Remedial action reports
- Violations of this CP or applicable CPS
- Revocation requests
- Subscriber identity authentication data as per Section 3.2.3
- Documentation of receipt and acceptance of certificates (if applicable)
- Subscriber agreements
- Documentation of receipt of tokens
- All CRLs issued and/or published
- Software and hardware (if appropriate) required to verify archive contents
- Documentation required by compliance auditors
- KES transactions
- Identification of the recipient of an escrowed key
- Reason for key recovery
- Verification of authorization for recovery of escrowed key
- KES security audit data

### 5.5.2 Retention Period of Archive

Archive records for shall be kept for a period of at least ten years, six months without any loss of data.

### 5.5.3 Protection of Archive

No unauthorized CAS or RA 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 transfer the archived data periodically to new media shall be defined by the archive site. No transfer of medium shall invalidate CAS or RA applied signatures. The CAS shall maintain a list of people authorized to modify or delete the archive, and make this list available during CP compliance audits. Sensitive archive information shall only be released in accordance with Section 9.4.

Archive media shall be stored in a separate, safe, secure storage facility. Prior to archive, archive records shall be labeled with the name of the CAS (for CAs, this shall be its Subject DN), the date, and the data sensitivity. Archive data shall be protected commensurate with the data that the archived escrowed keys provide access to.

### 5.5.4 Archive Backup Procedures

If a CNSS member agency chooses to back up archives, any backups shall be protected in the same manner as the original archives.

### 5.5.5 Requirements for Time-Stamping of Records

The archived record shall contain information necessary to allow the Security Auditor to determine when the event occurred. The time precision shall be such that the sequence of events can be determined. The CAS shall ensure that time stamps are consistent with an authoritative time standard.

### 5.5.6 Archive Collection System (Internal vs. External)

Archive data may be collected in any expedient manner.

### 5.5.7 Procedures to Obtain and Verify Archive Information

Each CAS shall document the procedures detailing how to create, package, transport, and verify their archive information. Only authorized CAS Operations Staff shall be allowed to access the archive.

## 5.6 KEY CHANGEOVER

See Section 6.1.4 for information on delivery of the Root CA certificate. See Section 2 for information on obtaining Intermediate and Subordinate CA certificates from the repository.

## 5.7 COMPROMISE AND DISASTER RECOVERY

### 5.7.1 Incident and Compromise Handling Procedures

If some form of potential compromise of a CA becomes known, the ANMA (or PMA in the case of the Root) shall perform an investigation in order to determine the nature and the degree of damage. If a CA private signing key is suspected of compromise, the procedures outlined in

Section 5.7.3 shall be followed. Otherwise, the scope of potential damage shall be assessed in order to determine if the CA needs to be rebuilt, only some certificates need to be revoked, and/or the CA private key needs to be declared compromised. The PMA shall make the determination that a Root CA private key has been compromised; the respective ANMA shall make the determination that an Intermediate or Subordinate CA private key has been compromised.

In case of a CSS key compromise, all certificates issued to the CSS shall be revoked and the revocation information shall be published immediately in the most expeditious manner. Subsequently, the CSS shall be re-keyed.

In the event that the KES is compromised or compromise is suspected, recovery procedures are required to return it to a secure state. If a compromise of the KES database is suspected, the ANMA shall be notified. The ANMA shall determine the extent of the compromise and direct the appropriate actions to reestablish a secure environment.

The ANMA shall notify the NSS PKI PMA if any of the following occur:

- Suspected or detected compromise of any CAS system or subsystem
- Physical or electronic penetration of any CAS system or subsystem
- Successful denial of service attacks on any CAS system or subsystem
- Any incident preventing a CA from issuing and publishing a CRL prior to the time indicated in the *nextUpdate* field in the currently published CRL

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

When computing resources, software, and/or data are corrupted, CASs operating under this policy shall respond as follows:

- Notify the ANMA as soon as possible
- Ensure that the system's integrity has been restored prior to returning to operation and determine the extent of risk due to operations since the last point of backup
- If the CA signing keys are not destroyed, the integrity of the system has been restored, and the risk is deemed negligible, reestablish CAS operations, giving priority to the ability to generate certificate status information within the CRL issuance schedule specified in Section 4.9.7
- If the CA signing keys are destroyed, the integrity of the system cannot be restored, or the risk is deemed substantial, reestablished CAS operations as quickly as possible, giving priority to the generation of a new CA signing key pair

### 5.7.3 Entity Private Key Compromise Procedures

In the case of the NSS PKI Root CA compromise, the NSS PKI PMA shall immediately notify all ANMAs, Agency POCs, and any cross-certified NSS PKIs of the Root CA compromise so that they can revoke any cross certificates issued to the Root CA or any Subordinate CAs and notify all Subscribers and Relying Parties to remove the trusted self-signed certificate from their trust stores. Initiation of notification shall be made in an authenticated and trusted manner at the earliest feasible time and shall not exceed 6 hours beyond determination of compromise or loss.

The NSS PKI PMA shall then re-establish the NSS PKI by generating a new Root CA certificate, issuing new Subordinate CA certificates, securely distributing the new Root CA certificate as specified in Section 6.1.4, and re-establishing any cross certificates.

In the event of an Intermediate or Subordinate CA key compromise, the issuing CA shall revoke that CA's certificate, and the revocation information shall be published immediately in the most expedient, authenticated, and trusted manner but within 18 hours after the notification. Subsequently, the CA shall be re-established as described in Section 5.7.4. The ANMA shall notify the NSS PKI of the CA key compromise. Upon re-establishment of the CA, new Subscriber certificates shall be issued. The ANMA shall also investigate and report to the NSS PKI PMA what caused the compromise or loss, and what measures have been taken to preclude recurrence.

In case of a CSS key compromise, the CA that issued the CSS a certificate shall revoke that certificate, and the revocation information shall be published immediately in the most expedient, authenticated, and trusted manner. The CSS shall subsequently be re-keyed. If the CSS is self-signed, the ANMA shall immediately notify the NSS PKI PMA, all ANMAs and Agency POCs, and any cross-certified PKIs of the CSS compromise so that they can notify all Subscribers and Relying Parties to remove trust in the CSS certificate from each Relying Party application, and install the re-keyed certificate.

In the event that the KES is compromised or compromise is suspected, recovery procedures are required to return it to a secure state. If a compromise of the KES database is suspected, the ANMA shall be notified. The ANMA shall determine the extent of the compromise and direct the appropriate actions to reestablish a secure environment. If the determination is made that the KES has been compromised, all compromised private keys within the KES shall be revoked, and the associated certificates re-issued.

In case of an RA key compromise, the CA that issued the RA a certificate shall revoke that RA's certificate, and the revocation information shall be published immediately in the most expedient, authenticated, and trusted manner. The compromise shall be investigated in order to determine the actual or potential date of the RA key compromise. All certificates approved by that RA since the date of actual or potential RA key compromise shall be revoked. A Security Auditor shall review the audit records for the KES to identify all potentially exposed escrowed keys. Certificates associated with all potentially exposed escrowed keys shall also be revoked.

In case of a TA key compromise, the CA that issued the TA a certificate shall revoke that TA's certificate, and the revocation information shall be published immediately in the most expedient manner. The compromise shall be investigated in order to determine the actual or potential date of the TA key compromise. All certificates issued involving the participation of the TA since the date of actual or potential TA key compromise shall be revoked. A Security Auditor shall review the audit records for the KES to identify all potentially exposed escrowed keys. Certificates associated with all potentially exposed escrowed keys shall also be revoked.

For Subordinate CAs, when a Subscriber certificate is revoked because of compromise, suspected compromise, or loss of the private key, a CRL shall be published at the earliest feasible time by the supporting CA, but in no case more than 6 hours after notification.

A CA using reason codes in CRLs, which identify the reason for revoking a certificate, shall have the ability to transition any reason code to compromise.

### 5.7.4 Business Continuity Capabilities after a Disaster

CASs are required to maintain a Disaster Recovery Plan.

In the case of a disaster in which the CAS equipment is damaged and inoperative, the CAS operations shall be re-established as quickly as possible, giving priority to the ability to revoke Subscriber's certificates. If the CAS cannot re-establish revocation capabilities prior to date and time specified in the *nextUpdate* field in the currently published CRL issued by the CA, then the inoperative status of the CAS shall be reported to the NSS PKI PMA. The NSS PKI PMA shall decide whether to declare the CA private signing key as compromised and re-establish the CA keys and certificates, or allow additional time for reestablishment of the CA's revocation capability.

In the case of a disaster whereby a CAS 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 CAS installation shall then be completely rebuilt by re-establishing the CAS 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 the data is forwarded, as no revocation information will be available (if the CRL signing key was destroyed).

## 5.8 CA, RA, OR TA TERMINATION

### 5.8.1 CA Termination

If the termination (complete cessation of operations) is for convenience, re-organization, or other non-security related reason, and provisions have been made to continue compromise recovery (including destruction or continued protection of the CA signing key), compliance and security audit, archive, revocation, and data recovery services, and all issued subscriber certificates are either expired or revoked, then neither the terminated CA's certificate nor certificates signed by that CA need to be revoked. If provisions for maintaining these services cannot be made, or subscriber certificates that have been issued will still be valid at the time of termination, then the CA termination will be handled as a CA compromise in accordance with Section 5.7.3.

For any CA termination, the responsible agency management authority (ANMA or PMA for the Root) shall maintain possession of any archive records and any security audit logs since the last archive.

### 5.8.2 RA Termination

If an RA is terminated for convenience, the RA's certificate shall be revoked and no other action is necessary. If an RA is terminated for negligence or there is other reason to believe that the RA's private key was used for unauthorized purposes, all certificates approved by that RA shall be revoked.

For any RA termination, another RA or the CAS shall take possession of any archive records and any security audit logs since the last archive maintained by that RA.

### 5.8.3 TA Termination

If a TA is terminated for convenience, the associated RA Officer will indicate that the TA is no longer approved as a TA and no other action is necessary.  If a TA is terminated for negligence or there is other reason to believe that the TA's private key was used for unauthorized purposes, all certificates approved by that TA since the beginning of the unauthorized or negligent activity shall be revoked and any data or logs will be maintained by the RA.

# 6 TECHNICAL SECURITY CONTROLS

## 6.1 KEY PAIR GENERATION AND INSTALLATION

### 6.1.1 Key Pair Generation

A private key is considered to be generated by the NSS PKI entity that first comes into possession of it: Subscriber, PKI Sponsor, RA, or CAS.

Pseudo-random numbers used for key generation shall be generated using a FIPS approved method.

A private key shall not appear outside of the module in which it was generated unless it is encrypted for transport (See Section 6.2.6) or, in the case of private keys associated with encryption certificates, for processing or storage by a key recovery mechanism.

Subscriber key pairs associated with certificates that assert the *id-CNSS-hardware* Policy OID may be generated outside the Subscriber hardware cryptographic module as long as they are generated on a NSA approved hardware cryptographic module and no copies, other than authorized escrowed copies of the private keys associated with Encryption certificates, continue to exist after the generation and insertion process has completed.

### 6.1.2 Private Key Delivery to Subscriber

If the PKI Sponsor generates the key pair locally within the cryptographic boundary of a cryptographic module, then there is no need to deliver the Subscriber’s private key, and this section does not apply.

If a private key is generated within or transferred to the hardware cryptographic module while the module is not in possession of the PKI Sponsor, then the hardware module shall be delivered to the PKI Sponsor in such a way that ensures the following:

- The correct token and activation data are provided to the correct PKI Sponsor
- No unauthorized parties can access or use the token during the delivery process

If a private key is generated in an external cryptographic module by a CAS or RA, the CAS or RA shall implement mechanisms to ensure that the key is securely delivered to the correct PKI Sponsor. Any transmission of a private key over a network or transfer from generation module to the Sponsor’s module shall use an encrypted and authenticated channel to the Subscriber’s cryptographic module.

In all cases, the following requirements shall be met:

- Any entity that generates a private key for a PKI Sponsor shall not retain any copy of the key after delivery of the private key, except for authorized key escrow of private keys associated with encryption certificates. All original copies of a plaintext private key shall be zeroized or destroyed in the generation module immediately upon encryption of the private key for delivery or extraction. An approved process shall ensure that additional copies cannot be made.

- The private key shall be protected from activation, compromise, or modification during the delivery process.
- The PKI Sponsor shall acknowledge receipt of the private key and/or the token, regardless of the delivery means. The CAS or RA shall maintain a record of the PKI Sponsor's acknowledgement of receipt. If the CAS or RA does not receive an acknowledgement of receipt within a specified time period, the CAS or RA shall revoke all relevant private keys. Tokens shall not be activated (published/enabled) until the Sponsor acknowledges receipt.
- For hardware cryptographic modules, accountability for the location and state of the module shall be maintained until the PKI Sponsor is in possession of it.
- For electronic delivery of private keys, the key material shall be transmitted or delivered to the PKI Sponsor in encrypted form, the encryption strength shall be commensurate with that of the key being protected, and the encryption method shall ensure that only the PKI Sponsor can decrypt and access the private keys.

### 6.1.3 Public Key Delivery to Certificate Issuer

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

### 6.1.4 CA Public Key Delivery to Relying Parties

The Root CA public key, and any other CA key used as a trust anchor, shall be distributed in a secure fashion. When the Root CA or other trust anchor CA signature key pair is updated, the new key shall likewise be distributed securely.

### 6.1.5 Key Sizes

Guidance on the selection of cryptographic algorithms and key sizes to support various levels of security can be found in *NIST Special Publication 800-57, Recommendation for Key Management – Part 1: General* [SP 800-57].

All certificates issued under this Policy shall contain public keys that can be employed in implementations requiring 112 bits of security, unless otherwise specified in Section 7.1.3.

The selection of cryptographic algorithms and key sizes used by the Transport Layer Security (TLS) protocol or any other protocol providing security services to accomplish the requirements of this CP shall support a minimum of 112 bits of security (e.g., Advanced Encryption Standard (AES)-128 in CBC mode for encryption and 2048-bit RSA keys for digital signatures).

CSSs shall sign responses using a signature algorithm, key size, and hash algorithm providing equal or greater bits of security as those used by the CA to sign CRLs.

### 6.1.6 Public Key Parameters Generation and Quality Checking

Public key parameters shall always be generated and checked in accordance with the standard that defines the crypto-algorithm in which the parameters are to be used. For example, public key parameters for use with algorithms defined in the *Federal Information Processing Standard 186-3, Digital Signature Standard* [FIPS 186] shall be generated and tested in accordance with [FIPS 186]. Whenever a crypto-algorithm is described in [FIPS 186], the parameter generation and checking requirements and recommendations of [FIPS 186] shall be required of all entities generating key pairs whose public components are to be certified by the CA.

Domain parameters shall be selected from those approved by NIST and NSA and within the Suite B set of algorithms as appropriate for the NSS PKI.

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

The use of a specific key is constrained by the k*eyUsage* extension in the X.509 certificate. All certificates shall include a critical k*eyUsage* extension.

Identity or signature certificates issued to Name Subscribers shall assert the *digitalSignature* bit. For CAs that support distinct identity and signature certificates, signature certificates but not identity certificates shall assert the *nonRepudiation* bit. For CAs that do not support distinct identity and signature certificates, identity certificates may assert the *nonRepudiation* bit. All other identity (e.g., Role Subscriber) certificates and all code signing certificates and content signing certificates shall only assert the *digitalSignature* bit. Encryption certificates shall only assert the *keyEncipherment* bit for RSA or *keyAgreement* for ECDH.

Certificates that only assert the *id-CNSS-device* Policy OID may be used for both digital signature and key management and may assert both the *digitalSignature* and *keyEncipherment* or *keyAgreement* bits as necessary to support legacy applications. Certificates that assert the *id-CNSS-software* or *id-CNSS-hardware* Policy OIDs shall not assert both the *digitalSignature* and *keyEncipherment* or *keyAgreement* bits.

Public keys that are bound into CA certificates shall be used only for signing certificates and status information (e.g., CRLs). CA certificates whose subject public key is to be used to verify other certificates shall assert the *keyCertSign* bit. CA certificates whose subject public key is to be used to verify CRLs shall assert the *cRLSign* bit. CSS certificates whose subject public key is to be used to verify OCSP responses shall assert the *digitalSignature* and/or *nonRepudiation* bits.

The *dataEncipherment*, *encipherOnly*, and *decipherOnly* bits shall not be asserted in certificates issued under this CP.

## 6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

### 6.2.1 Cryptographic Module Standards and Controls

All cryptographic modules and associated middleware (as part of the module implementation) shall be approved by NSA specifically for use on a SECRET network in association with the NSS PKI, in accordance with [CNSSP 25].

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 a cryptographic module.

For certificates that assert the *nonRepudiation* bit, no one shall have access to the private signing key but the PKI Sponsor named in the certificate. Any private keys associated with encryption certificates escrowed by a CAS shall be held in strictest confidence only by those parties authorized by this policy and controlled as described in this CP.

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

A single person shall not be permitted to activate a CA or CSS signature key or access any cryptographic module containing the complete private signing key. Access to CAS keys backed up for disaster recovery shall be under the same multi-person control as the original CAS key. The names of the CAS Operations Staff 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 any party other than the named PKI Sponsor.

For purposes such as data recovery, it is necessary to provide for recovery of private keys associated with encryption certificates. To facilitate this, the CAS shall offer a key escrow and recovery capability.

### 6.2.4 Private Key Backup

For *id-CNSS-hardware*, PKI Sponsors are not permitted to backup or otherwise copy their own private keys. Subscriber private signature and identity keys shall not be backed up or copied. See Section 6.2.3 for encryption private key escrow.

For *id-CNSS-software*, PKI Sponsors are permitted to make a backup of their own private keys. However, backup copies of private keys shall be stored only on removable media and shall not be stored online. All copies of backup private keys shall be continuously protected by the PKI Sponsor at least commensurate with the level of the data the key provides access to or protects as outlined in Section 6.2.7.

For *id-CNSS-device*, PKI Sponsors are permitted to make operational copies of private keys for each application that requires the key in a different location or format; however, private keys stored in each of these applications or locations shall be in cryptographic modules that have been approved by NSA. All key transfers shall be done from an approved cryptographic module, and the key shall be encrypted during the transfer. The PKI Sponsor is responsible for ensuring that all copies of private keys, including those that might be embedded in system or device backups, are protected, including protecting any workstation on which any of its private keys reside.

CA private keys shall be backed up under the same multi-person control as the original private keys. The number of backup copies shall be limited to the number required to ensure the availability of the key in the event of disasters, operational failures, or other unforeseen circumstances. Cryptographic modules used to store backup copies shall meet all cryptographic module requirements for the CA.

### 6.2.5 Private Key Archival

CA private signing keys and private keys associated with certificates other than encryption certificates shall not be archived. CASs that retain private keys associated with encryption certificates shall archive such keys in accordance with Section 5.5.

See also Section 6.2.3 and Section 6.2.4.

### 6.2.6 Private Key Transfer into or from a Cryptographic Module

Private keys shall 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 shall be encrypted during transport. The strength of the encryption process shall be commensurate with the key being transported. The encryption process shall ensure that only the authorized party(ies) can decrypt the transported key. Private keys shall never exist in plaintext form outside a cryptographic module boundary.

Private or symmetric keys used to decrypt other private or symmetric keys for transport or storage (including key escrow) shall be protected from disclosure. The cryptographic strength of, and protection afforded to, these keys shall be commensurate with that of the keys being encrypted in accordance with Section 6.1.5 and Section 6.4.1.

### 6.2.7 Private Key Storage on Cryptographic Module

The private key stored in the cryptographic module shall be protected from unauthorized access and use in accordance with *Federal Information Processing Standard 140, Security Requirements For Cryptographic Modules* [FIPS 140] and NSA requirements applicable for the module. Cryptographic modules and other media containing private key shall be handled and stored as specified in Sections 5.1.2 and 5.1.6.

### 6.2.8 Method of Activating Private Key

Passwords, biometric data, or other mechanisms of equivalent authentication robustness shall be used to activate the private key in a cryptographic module. See Section 6.4.1 for activation data generation requirements. Activation data may be distributed in person, or provided to the PKI Sponsor separately from the cryptographic modules that they activate. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

### 6.2.9 Method of Deactivating Private Key

Cryptographic modules that have been activated shall be protected against unauthorized access. After use, the cryptographic module shall be deactivated (e.g. via a manual logout procedure or automatically after a period of inactivity by a passive timeout). Hardware cryptographic modules shall be removed and stored in accordance with Section 5.1.2 when not in use.

### 6.2.10 Method of Destroying Private Key

Private keys associated with identity, signature, code signing, content signing, or system or device certificates that do not assert *keyEncipherment* or *keyAgreement* shall be destroyed and any keys used to transport them, where possible, when the certificates to which they correspond expire or are revoked. Private keys associated with encryption certificates shall be destroyed when they are no longer needed. For software cryptographic modules, this may be by overwriting the data. For hardware cryptographic modules, this may be through executing a zeroize command. Physical destruction of hardware cryptographic modules should not be required. Methods used for the destruction of keys shall be approved by NSA.

### 6.2.11 Cryptographic Module Rating

See Section 6.2.1.

## 6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

### 6.3.1 Public Key Archival

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

### 6.3.2 Certificate Operational Periods and Key Pair Usage Periods

A CA uses its signing key for creating certificates. However, Relying Parties employ the CA certificate for the life of any certificates signed by that CA beyond that signing. Therefore, CAs shall not issue certificates that extend beyond the expiration date of their own certificates and public keys. The CA private key shall be used to sign CRLs until all certificates signed by it have also expired. The CA key period shall not be shorter than the end entity period of any certificates that it issues.

The following table provides the maximum validity period of keys and certificates and use period of the private keys associated with the public keys in those certificates. Certificates using cryptographic algorithms of less than 128-bits of security shall not be valid beyond 31 December 2030.

**Table 6-1: Key and Certificate Validity Periods**

| Certificate Type | Key Validity Lifetime | Certificate Validity | Key Usages |
|---|---|---|---|
| Root CA | 25 years | 25 years | 20 years to sign certificates<br>25 years to sign CRLs |
| Intermediate CA (Operated Off-line) | 25 years | 25 years | 20 years to sign certificates<br>25 years to sign CRLs |
| Intermediate CA (Operated On-line) | 10 years | 10 years | 9 years to sign certificates<br>10 years to sign CRLs |
| Subordinate CA | 10 years | 10 years | 9 years to sign certificates<br>10 years to sign CRLs |
| CSS (Delegated Model with noCheck) | 3 years | 1 month | 1 month |
| CSS (Delegated model without noCheck) | 3 years | 3 years | 3 years |

| **Certificate Type** | **Key Validity Lifetime** | **Certificate Validity** | **Key Usages** |
|---|---|---|---|
| CSS (Explicit trust model) | 3 years | 3 years | 3 years |
| Other CAS Components | 3 years | 3 years | As long as needed |
| Identity (*id-CNSS-software*)† | 1 years | 1 years | 1 years |
| Signature (*id-CNSS-software*)† | 1 years | 1 years | 1 years |
| Encryption (*id-CNSS-software*)† | 1 years | 1 years | As long as needed‡ |
| Identity | 3 years | 3 years | 3 years |
| Signature | 3 years | 3 years | 3 years |
| Encryption | 3 years | 3 years | As long as needed‡ |
| Code Signing | 8 years | 8 years | 3 years |
| Content Signing | 8 years | 8 years | 3 years |
| System or Device | 3 years | 3 years | 3 years |

† Certificates used to support individuals in disadvantaged environments may possess a validity equivalent to the sponsor’s length of deployment plus 3 months, but not to exceed a 3 year maximum with PMA approval.

‡ Encryption certificates shall not be used to encrypt new data beyond the certificate validity date; however, they may be used to decrypt data previously encrypted.

## 6.4 ACTIVATION DATA

### 6.4.1 Activation Data Generation and Installation

Guidance on activation data generation and installation can be found in [FIPS 140].

A pass-phrase, Personal Identification Number (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 [FIPS 140].

Pass-phrases or PINs shall be randomly generated when possible. If random numbers are used to generate PINs or pass-phrases, they shall meet all the applicable [FIPS 140] 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 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).

Activation data may be selected by the PKI Sponsor or RA. Activation data shall only be selected by the RA if the keys are generated remotely from the PKI Sponsor. If activation data is selected by the RA, the PKI Sponsor shall change activation data upon initial receipt.

PKI Sponsors or RAs who create pass-phrases or PINs shall be instructed to select activation data that is not related to their personal identity, history, or environment. Sequences, repeated characters or numbers, social security numbers, dictionary words or names, date formats, or other easily guessed numbers shall not be used. To the extent practicable, technical means shall be used to verify that the activation data meets all of the requirements in this section. When alphanumeric pass-phrases are used, an interspersed mix of eight 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 one to four digits. The activation data shall not contain sequences, repeated characters, date formats, or license plate formats. To the extent practicable, technical means shall be used to verify that the activation data meets all of the requirements in this section.

### 6.4.2 Activation Data Protection

Activation data for cryptographic modules should be memorized, not written down. If it is written down, it shall be classified as SECRET and secured appropriately, and shall not be stored with the cryptographic module.

Activation data for private keys associated with Name certificates shall never be shared. Activation data for private keys associated with Role, or System or Device certificates shall be restricted to those authorized to use the private keys.

Activation data for recovered copies of escrowed keys shall only be provided from the KES or RA to the authenticated and authorized requestor.

Activation data shall be afforded protection at a minimum commensurate with the classification of the data that the key that it activates provides access to.

### 6.4.3 Other Aspects of Activation Data

If activation data is transmitted, it shall be via an appropriately protected channel, which is distinct in time and place from the associated cryptographic module. If transmission is not done by hand, the PKI Sponsor shall be advised of the shipping date, method of shipping, and expected delivery date of any activation data. As part of the delivery method, PKI Sponsors will sign and return a delivery receipt. In addition, PKI Sponsors shall also receive an Acknowledgement of Responsibilities form that identifies specifics and provides guidance for protection of the activation data.

Any electronic secure channel for delivery of activation data or shared secret (e.g., password) shall be of strength commensurate with the private key being protected and ensure that only the PKI Sponsor can decrypt it. Any physical delivery shall be via a continuously accountable means that ensures that only the PKI Sponsor receives the activation data.

CASs and RAs shall change their cryptographic module activation data whenever their certificates are re-keyed.

## 6.5 COMPUTER SECURITY CONTROLS

### 6.5.1 Specific Computer Security Technical Requirements

CAS, RA and Repository systems and operating systems shall be configured in accordance with all relevant NSA Configuration Guides and STIGs or local agency equivalent.

CAS components and RA workstations shall operate with the minimal number of accounts required for administration and operation.

For CAS and RA components, either remote management and login shall be disabled, or remote maintenance shall be conducted via an end-to-end (administrator machine to component) virtual private network using cryptography commensurate with the strength of the NSS PKI keys being issued. Network protocols not required for CAS or RA operation or remote administration shall be disabled. TELNET and File Transfer Protocol (FTP) shall never be enabled.

CAS equipment shall support the following:

- Archive CAS history and audit data
- Authenticate the identity of users before permitting access to the system or applications
- Enforce access control for CAS services and NSS PKI roles
- Enforce domain integrity boundaries for security-critical processes (i.e., operating system self protection and process isolation)
- Enforce separation of duties for NSS PKI roles
- Generate and archive audit records for all transactions (see Section 5.4)
- Manage privileges of users to limit users to their assigned roles
- Prohibit object reuse or require separation for CAS random access memory
- Provide discretionary access control
- Require a trusted path for identification and authentication of NSS PKI roles and associated identities
- Require self-test security-related CAS services
- Require use of cryptography for session communication and database security
- Support recovery from key or system failure

### 6.5.2 Computer Security Rating

No stipulation.

## 6.6 LIFE CYCLE TECHNICAL CONTROLS

### 6.6.1 System Development Controls

CASs and RAs shall use software that has been designed and developed under a formal, documented development methodology, such as Capability Maturity Model Integration (CMMI).

Hardware and software procured to operate CAS or RA systems shall be purchased and shipped in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).

Hardware and software developed specifically for the PKI shall be developed in a controlled environment, and the development process shall be defined and documented.

### 6.6.2 Security Management Controls

Hardware and software shall be dedicated to performing the functions of the CAS and RA. All installed applications, hardware devices, network connections, or component software shall be necessary to CAS or RA operations.

The configuration of CAS and RA systems, as well as any modifications and upgrades, shall be documented and controlled. CAS and RA systems shall not have installed applications or component software that are not part of CAS and RA configurations. There shall be a mechanism for detecting unauthorized modification to the software or configuration. A formal configuration management methodology shall be used for installation and ongoing maintenance of CAS and RA systems. There shall be a mechanism for detecting unauthorized modifications to the CAS and RA system software or configuration.

CAS and RA software, when first loaded, shall be verified as being that supplied from the vendor, with no modification, and be the version intended for use. The CAS and RA shall periodically verify the integrity of the software.

### 6.6.3 Life Cycle Security Controls

Proper care shall be taken to prevent malicious software from being loaded onto CAS or RA equipment. Hardware and software shall be scanned for malicious code on first use and periodically thereafter.

Chain of custody mechanisms that provide continuous accountability shall be provided throughout the lifecycle of the system, to include shipment and delivery of hardware and software from the purchase location to the CAS or RA physical location; creation, storage, transport, or manipulation of CAS key material; and physical or logical access to CAS or RA systems.

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

CAS equipment and any CAS tokens shall be shipped via a method providing security equivalent to 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. NSS PKI equipment (hardware and software) shall not be considered or labeled COMSEC or CRYPTO material. PKI, while not COMSEC material, should be protected to comparable standards. (See CNSS 4005.) Local requirements shall also be in effect.

## 6.7 NETWORK SECURITY CONTROLS

Online CAS and RA equipment shall be classified SECRET and reside on a SECRET network.

CAS and RA equipment shall be located on internal networks behind boundary/perimeter network defenses. Services allowed to and from the CAS or RA equipment shall be limited to those required to perform CAS or RA functions. A firewall shall be implemented that contains the following security features:

- Audit of security events
- Protection of security audit log

- Identification & Authentication with Secure Action Upon Authentication Failure
- If data is communicated with Intrusion Detection System (IDS) components, confidentiality and integrity of this data
- Non-by-passable and self protection
- Ability to filter packets based on source, destination, and port number

The PKI ANMAs shall employ network security controls to protect CASs and Repositories. The ANMA shall assure that all CAS equipment is protected (e.g., network guard, firewall, and/or filtering router) against known network attacks. CAS Operations Staff shall turn off all unused network ports and services on the CASs, and ensure that similar measures are taken on all guards, routers, and firewalls. Any network software present on CAS equipment shall be necessary to the functioning of the CAS application.

Boundary control devices shall be used to protect the network on which CAS equipment is hosted; and, shall deny all but the necessary services to the CAS equipment even if those services are enabled for other devices on the network. Boundary control devices shall only be configured with the minimum user accounts required for their operation, and shall be configured to reject a packet originating outside the network that is using an address from the range used by internal networks.

## 6.8 TIME STAMPING

CASs shall regularly synchronize with an authorized time source. Time derived from the time source shall be used for establishing the time of certificate issuance, CRL issuance, OCSP responses, and audit logs.

# 7 CERTIFICATE, CRL, AND OCSP PROFILES

## 7.1 CERTIFICATE PROFILE

### 7.1.1 Version Number(s)

CAs shall issue [ITU X.509] version 3 certificates only.

### 7.1.2 Certificate Extensions

Rules for the inclusion, assignment of value, and processing of extensions are defined in [NSS PKI PROF]. Any variance to these profiles shall be approved by the NSS PKI Member Governing Body.

### 7.1.3 Algorithm Object Identifiers

Certificates under this Policy will use OIDs from the following table for signatures. CAs shall use at least SHA-1 hash algorithm when generating digital signatures. The NSS PKI PMA, at the recommendation of the NSS PKI Member Governing Body, shall determine the timeframe for migration away from SHA-1 to a minimum of SHA-256.

**Table 7-1: Certificate Signature OIDs**

| Name | OID |
|---|---|
| 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} |
| id-RSASSA-PSS | {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10} |
| ecdsa-with-SHA1 | {iso(1) member-body(2) us(840) ansi-x9-62 (10045) signatures (4) 1 } |
| ecdsa-with-SHA256 | {iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2} |
| ecdsa-with-SHA384 | {iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3} |

Where certificates are signed using RSA with PSS padding, the OID is independent of the hash algorithm; the hash algorithm is specified as a parameter. RSA signatures with PSS padding may be used with the hash algorithms and OIDs specified in the table below.

**Table 7-2: Hash OIDs**

| Name | OID |
|---|---|
| id-sha256 | {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1} |

Certificates under this Policy will use OIDS from the following table for identifying the algorithm for which the subject key was generated.

**Table 7-3: Key Generation OIDs**

| Name | OID |
|---|---|
| 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} |
| id-ecDH | {iso(1) identified-organization(3) certicom(132) schemes(1) ecdh(12)} |
| rsaEncryption | {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1} |

Where certificates contain an elliptic curve public key, the parameters shall be specified as one of the curves named in the following table.

**Table 7-4: Elliptic Curve OIDs**

| Name | OID |
|---|---|
| ansip256r1 (a.k.a x962p256r1) | {iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7} |
| ansip384r1 (a.k.a x962p384r1) | {iso(1) identified-organization(3) certicom(132) curve(0) 34} |

In order to provide cryptographic separation for a closed community, when the subject public key is of the form id-ecDH, a private OID may be asserted to indicate a different base point on one of the above curves.

CAs shall certify only public keys associated with the crypto-algorithms identified above, and shall only use the signature crypto-algorithms described above to sign certificates, CRLs and any other NSS PKI product, including other forms of revocation information such as OCSP responses.

### 7.1.4 Name Forms

In general, the DN will be used for lookups. All CAs 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 *Subject Alternative Name* extension. Any name form defining GeneralName in *X.500: Information Technology - Open Systems Interconnection - The Directory: Overview of Concepts, Models and Services* [ITU X.500] may be used, in accordance with the required profile in [NSS PKI PROF].

For attribute values other than Domain Component (dc), all CA Distinguished Names (in various fields such as *issuer*, *subject*, *subjectAlternativeName*, *nameConstraints*, etc.) shall be encoded as printable string. All Subscriber DN portions, that name constraints apply to, shall be encoded as printable string. Other portions of the Subscriber DN shall be encoded as printable string if possible. If a portion cannot be encoded as printable string, then and only then, shall it be encoded using a different format and that format shall be Unicode Transformation Format (UTF) 8.

For dc attribute values, all dc attribute values shall be encoded as International Alphabet (IA) 5 string.

### 7.1.5 Name Constraints

Where feasible, name constraints shall be technically enforced.

### 7.1.6 Certificate Policy Object Identifier

Certificates issued under this policy shall assert one or more of the Certificate Policy OIDs defined in Section 1.2.

### 7.1.7 Usage of Policy Constraints Extension

CA signing certificates shall contain a non-critical *policyConstraints* extension with skipCerts=0 for the *requireExplicitPolicy* field.

### 7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued under this policy may contain the following policy qualifiers.

- User notice
- CP/CPS pointer

### 7.1.9 Processing Semantics for the Critical Certificate Policies Extension

This policy does not require the *certificatePolicies* extension to be critical. Relying Parties that do not process this extension do so at their own risk.

## 7.2 CRL PROFILE

### 7.2.1 Version Number(s)

CAs shall issue [ITU X.509] version 2 CRLs only.

### 7.2.2 CRL and CRL Entry Extensions

The CRL shall always populate the *nextUpdate* field. Complete profiles for CRLs issued by the NSS PKI can be found in [NSS PKI PROF].

## 7.3 OCSP PROFILE

### 7.3.1 Version Number(s)

CSSs shall use OCSP Version 1.

### 7.3.2 OCSP Extensions

OCSP Profile information can be found in [NSS PKI PROF].

Appropriate extensions from *IETF X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP* [RFC 2560] may be used in OCSP requests and responses. If a request contains a nonce and the response does not contain the nonce, the Relying Party may process the response if the information is deemed reasonably current.

# 8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

## 8.1 FREQUENCY AND CIRCUMSTANCES OF ASSESSMENT

All CASs shall conduct an initial compliance audit prior to receiving their CA signing certificate indicating that they are prepared to operate in compliance with all CP and CPS requirements. The initial compliance audit shall include a review of RA system design.

At least once every three years, each ANMA, including the ANMA operating the Root CA, shall conduct a full compliance audit and submit an audit report to the NSS PKI Member Governing Body. In the interim, an annual assertion of the completion of an alternative review may be submitted in lieu of a full compliance audit report if the most recent full compliance audit had no significant findings, and no changes to policies, procedures, or operations have occurred since the last full compliance audit.

At least once every three years, RA Officers shall be subject to a full compliance audit by the appropriate ANMA. If any of the following are true, RAs Officers shall be audited within a year of the last audit or of the occurrence of the situation:

- The previous RA Officer audit report contained discrepancies
- The RA Officer role experienced personnel turn-over
- Changes have been made to the CPS or RPS that affect RA Officer operations

The NSS PKI PMA and NSS PKI Member Governing Body have the right to require aperiodic compliance audits of CASs, RAs, or TAs operating under this policy. The NSS PKI PMA or Member Governing Body shall state the reason for any aperiodic compliance audit.

## 8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

The compliance auditor shall demonstrate competence in the field of security compliance audits and shall be thoroughly familiar with the applicable CPS. The compliance auditor shall perform CA or information system compliance audits as a regular ongoing business activity. In addition, the compliance auditor shall have expertise in information security, cryptography, and NSS PKI who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

The NSS PKI PMA may request the bona fides of any compliance auditor, indicating that the auditor meets the specified requirements. The NSS PKI Member Governing Body may review the bona fides of compliance auditors as an integral part of the compliance audit review process.

## 8.3 ASSESSOR’S RELATIONSHIP TO ASSESSED ENTITY

The compliance auditor shall either be a private firm that is independent from the entity being audited, or shall be sufficiently separated organizationally from the entity to provide an unbiased, independent evaluation. This relationship shall clearly demonstrate the independence of the compliance auditor from the entity operating or managing the NSS PKI. The compliance auditor shall not have developed or maintained the CAS, the CAS facility or the CPS for the entity being audited.

## 8.4 TOPICS COVERED BY ASSESSMENT

### 8.4.1 Initial Compliance Audit

The compliance audit shall verify that the CAS is prepared to operate in compliance with this CP and its CPS. This initial audit shall verify that all provisions of the approved CPS that can be determined prior to commencing operations have been met.

### 8.4.2 Full Compliance Audit

The compliance audit shall verify that all provisions of the approved CPS or RPS have been implemented.

The purpose of the compliance audit shall be to verify that the audited party has in place a system to assure the quality of the services that it provides, and that it complies with all the requirements of the current versions of this CP and its CPS or RPS. All aspects of the audited party's operation related to this CP and its CPS or RPS shall be subject to compliance audit inspections.

The ANMA shall ensure that the audit report provides the following information at a minimum. In order to evaluate compliance and the compliance audit, the following background information regarding the compliance auditor is required:

- Identity of the compliance auditor and the individuals performing the audit
- Competence of the compliance auditor to perform audits
- Experience of the individuals performing the audit in auditing NSS PKI systems
- Relationship of the compliance auditor to the entity that owns the NSS PKI

The following information regarding the audit itself is required:

- The date the audit was performed
- The formal or informal methodology used
- Which documents were reviewed as a part of the audit, including document dates and version numbers

In addition to this background, the entity should ensure that, as part of the audit, an audit summary is prepared, signed by the auditor, reporting on the following elements after conducting the compliance audit:

- State the scope of the audit
- State that the operations of CAS or RA were evaluated for conformance to the requirements of its CPS or RPS, and any applicable MOAs
- Report the findings of the evaluation of operational conformance to the CPS, RPS, and/or MOAs
- For the Root CA or Intermediate CAs, state whether current audit reports showing compliance were on file for any Subordinate CAs

### 8.4.3 Alternative Review

For the alternative review, the ANMA shall submit an assertion that no changes to policies procedures, operations, or systems have occurred, and that a compliance auditor has reviewed the following for compliance with the CPS:

- Personnel controls
- Separation of duties
- Audit review frequency and scope
- Types of events recorded in physical and electronic audit logs
- Protection of physical and electronic audit data
- Physical security controls
- Backup and archive generation and storage

## 8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

When the compliance auditor finds a discrepancy between the operations of a CAS or RA and the stipulations of its CPS or RPS, the following actions shall occur:

- The compliance auditor shall note the discrepancy
- The compliance auditor shall notify the parties identified in Section 8.6 of the discrepancy
- The audited party shall propose a remedy, including expected time for completion, to the ANMA.
- The ANMA shall review the proposed remedies and timelines to determine if they are sufficient.
- The ANMA shall determine what further notifications or actions are necessary to meet the requirements of this CP, or the CPS or RPS, and then proceed to make such notifications without delay

If the compliance auditor finds a critical failure that contributes to the ongoing compromise of information, the compliance auditor shall immediately report the issue to both the local authority, the ANMA, and to the Member Governing Body on behalf of the NSS PKI PMA 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 the following:

- Detection of a successful attempt to compromise classified or sensitive information
- Detection of an overt and intentional disregard for secure operations of the system
- Detection of systematic or widespread negligence in meeting requirements of the CPS or RPS
- Detection of any instance of negligence or error that could have led to a serious compromise or security breach
- Detection of a system configuration that causes the wide-spread public dissemination of classified or sensitive information

If any substantive or critical discrepancies are found, the CAS or RA shall be subject to a follow-up audit to confirm the implementation and effectiveness of the remedy.

## 8.6 COMMUNICATION OF RESULTS

For CAS audits, the compliance auditor shall report the results of the audit to the ANMA, and to the Member Governing Body on behalf of the NSS PKI PMA. For RA audits, the compliance auditor shall report the results of the audit to the ANMA and the Agency POC for the member agency of the RA. The auditor shall also communicate the implementation of any remedies to the ANMA, and to the Member Governing Body on behalf of the NSS PKI PMA. The ANMA or the Member Governing Body on behalf of the NSS PKI PMA will determine the appropriateness of the remedy and may take additional measures as defined in Section 8.5.

# 9 OTHER BUSINESS AND LEGAL MATTERS

## 9.1 FEES

### 9.1.1 Certificate Issuance or Renewal Fees

No stipulation.

### 9.1.2 Certificate Access Fees

No stipulation.

### 9.1.3 Revocation or Status Information Access Fees

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

### 9.1.4 Fees for Other Services

Consistent with applicable Federal law, Federal entities and their designees providing authorized NSS PKI services may reserve the right to charge a fee to member agencies and external entities in order to support the operations of the NSS PKI, including the Root CA and central repository. The Federal entities and their designees providing authorized NSS PKI services will use these fees only to fund operation of the NSS PKI, based on the recommendation of the NSS PKI Member Governing Body.

### 9.1.5 Refund Policy

No stipulation.

## 9.2 FINANCIAL RESPONSIBILITY

Relying Parties should determine, within their purview, what financial limits if any they wish to impose for the reliance on certificates used to consummate a transaction; and shall implement applications as appropriate to support those limitations. The NSS PKI PMA and other elements within the CNSS assume no financial responsibility or liability for those decisions in accordance with the *Federal Tort Claims Act* [FTCA].

### 9.2.1 Insurance Coverage

No stipulation.

### 9.2.2 Other Assets

No stipulation.

### 9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

### 9.2.4 Fiduciary Relationships

Issuance of certificates in accordance with its CPS does not make CAS Operations Staff, or any RA Officer or TA, an agent, fiduciary, trustee, or other representative of PKI Sponsors or Relying Parties.

## 9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

### 9.3.1 Scope of Business Confidential Information

Not applicable. See Section 9.4 for privacy requirements.

### 9.3.2 Information Not Within the Scope of Business Confidential Information

Not applicable. See Section 9.4 for privacy requirements.

### 9.3.3 Responsibility to Protect Business Confidential Information

Not applicable. See Section 9.4 for privacy requirements.

## 9.4 PRIVACY OF PERSONAL INFORMATION

### 9.4.1 Privacy Plan

Collection of personal information during identity authentication may be subject to collection, maintenance, retention, and protection requirements of *5 U.S.C. 552a, Privacy Act of 1974* [PRIVACT].

The NSS PKI PMA and member ANMAs shall conduct a Privacy Impact Assessment. If deemed necessary, the NSS PKI PMA and member ANMAs shall have a Privacy Plan to protect personally identifying information from unauthorized disclosure. The respective member agency Privacy Officer shall approve the Privacy Plan.

### 9.4.2 Information Treated as Private

CASs, RAs, and TAs shall protect all PKI Sponsor personally identifying information that is collected but not included in certificates from unauthorized disclosure. CASs shall also protect personally identifying information collected to support subordination, cross certification, and/or MOA requirements from unauthorized disclosure. CASs, RAs, and TAs shall handle all such information as sensitive, and access shall be restricted to those with an official need-to-know in order to perform their official duties.

Private keys shall be held in strictest confidence. Private keys generated by the CAS or escrowed by the CAS shall never appear unencrypted outside the CAS equipment.

### 9.4.3 Information Not Deemed Private

A certificate should only contain information that is relevant and necessary to effect transactions with the certificate. Information included in certificates, CRLs, and certificate status requests and responses shall not be deemed private, and is not subject to the protections outlined in the other subsections of Section 9.4.

### 9.4.4 Responsibility to Protect Private Information

Any keys held by a CAS shall be released only to an organizational authority, in accordance with the CPS, organizational policy, and this policy, or a law enforcement official, in accordance with U.S. law and this policy (see Section 9.4.6).

Collection of personal information may be subject to collection, maintenance, retention, and protection requirements of [PRIVACT]. All information 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.

In order to preserve trust in the NSS PKI, information concerning the events leading up to a revocation, or an investigation of a possible revocation shall be limited to those parties involved.

### 9.4.5 Notice and Consent to Use Private Information

A CAS is not required to provide any notice or obtain the consent of the PKI Sponsor in order to release private information.

### 9.4.6 Disclosure Pursuant to Judicial or Administrative Process

A CAS shall not disclose certificate or certificate-related information to any third party except in the following cases:

- When authorized by this CP or its CPS
- When required to be disclosed by law, governmental rule or regulation, or by order of a court of competent jurisdiction
- When authorized by the PKI Sponsor when necessary to effect an appropriate use of the certificate

CASs, RAs, and TAs shall process any request for release of information according to *41 CFR 105-60.605 - Procedure in the Event of a Demand for Production or Disclosure* [41 CFR 105-60.605].

### 9.4.7 Other Information Disclosure Circumstances

CASs may release records of individual transactions upon request of any PKI Sponsor involved in the transaction, or their legally recognized agents. A CAS shall not release the contents of archives maintained by CASs operating under this policy except as required by law.

## 9.5 INTELLECTUAL PROPERTY RIGHTS

An ANMA shall retain ownership and all intellectual property rights for any public key certificates that it issues. The sponsoring CNSS member agency shall retain ownership and all intellectual property rights for all private keys associated with certificates issued by any NSS PKI CA. CAs shall not knowingly violate intellectual property rights held by others.

## 9.6 REPRESENTATIONS AND WARRANTIES

### 9.6.1 CAS Representations and Warranties

CASs operating under this policy shall warrant that their procedures are implemented in accordance with this CP, and that any certificates issued that assert the policy OIDs identified in this CP were issued in accordance with the stipulations of this policy. A CAS who is found to have acted in a manner inconsistent with these obligations is subject to action by the NSS PKI Member Governing Body or by the Root CA. This action may include revocation of the subordinate or cross certificate issued to that CAS.

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

- Providing to the NSS PKI PMA a CPS, as well as any subsequent changes, for conformance assessment
- Conforming to the stipulations of this CP and the approved CPS
- Ensuring that registration information is accepted only from CA Operations Staff or RA Officers who understand and are obligated to comply with this policy
- Including only valid and appropriate information in certificates, and maintaining evidence that due diligence was exercised in validating the information contained in the certificates
- Revoking the certificates of Subscribers whose PKI Sponsor have been found to have acted in a manner counter to their obligations in accordance with Section 9.6.3
- Operating or providing for the services of an on-line repository that satisfies the obligations in Section 2, and informing the repository service provider of these obligations if applicable
- Posting certificates and CRLs to the repository
- Protecting escrowed copies of private keys from unauthorized disclosure

A CAS that operates a CSS shall ensure the following:

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

### 9.6.2 RA Representations and Warranties

An RA that performs registration functions as described in this policy shall comply with the stipulations of this policy, and comply with a CPS approved by the NSS PKI PMA or RPS approved by the appropriate ANMA 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 the RA certificate, termination of RA responsibilities by the sponsoring agency, and potentially adverse administrative or disciplinary action under Agency regulations. An RA supporting this policy shall conform to the stipulations of this document, including the following:

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

### 9.6.3 PKI Sponsor Representations and Warranties

A PKI Sponsor shall be required to sign a document containing the requirements the PKI Sponsor shall meet respecting protection of the private key and use of the certificate before being issued the certificate.

PKI Sponsors shall do the following:

- Accurately represent themselves in all communications with NSS PKI authorities
- Protect their private keys at all times, in accordance with this CP, as stipulated in their certificate acceptance agreements, and local procedures
- Promptly notify an RA Officer or TA upon suspicion of loss or compromise of their private keys—such notification shall be made directly or indirectly through mechanisms consistent with the CAS's CPS
- Promptly notify an RA Officer or TA of any changes to the information contained in their certificates
- Abide by all the terms, conditions, and restrictions levied upon the use of their private keys and certificates
- Upon notification of the recovery of an escrowed private key, determine if revocation of the associated certificate is necessary, and request the revocation if needed
- Ensure that each individual accessing a Role Certificate also possesses an individual Name Certificate
- Ensure that no individual continues to have access to the Role Certificate private key after leaving the role or relinquishing the role's authority
- Maintain a list of all persons authorized access to the Role or Device Certificate, to include the dates/times of such access, and make the list available for audit

### 9.6.4 Relying Party Representations and Warranties

Relying Parties who rely upon the certificates issued under a policy defined in this document should do the following:

- Use the certificate for the purpose for which it was issued, as indicated in the certificate
- Verify that the certificate has not been revoked prior to reliance

If Relying Parties fail to use certificates for their stated purpose or use certificates without verifying the revocation status information, this CP makes no representations or warranties regarding those certificates.

### 9.6.5 Representations and Warranties of Other Participants

#### *9.6.5.1 Repository Representations and Warranties*

Repositories that support a CAS in posting information as required by this policy shall perform the following:

- 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 specified in Section 2.4

#### *9.6.5.2 NSS PKI PMA*

The NSS PKI PMA shall do the following:

- Approve the CPS for each CA that issues certificates under this policy
- Review periodic compliance audits to ensure that CASs are operating in compliance with their approved CPSs
- Review name space control procedures to ensure that distinguished names are uniquely assigned for all certificates issued under this CP
- Revise this CP to maintain the level of assurance and operational practicality
- Distribute this CP to CNSS member agencies
- Coordinate modifications to this CP to ensure continued compliance by CASs operating under approved CPSs

#### *9.6.5.3 ANMA*

An ANMA shall do the following:

- Review periodic compliance audits to ensure that CASs, RAs, and other components operated by the agency are operating in compliance with their approved CPSs
- Review name space control procedures to ensure that distinguished names are uniquely assigned within their agency
- Ensure that any CAS Operations Staff, RA Operations Staff including RA Officers, TAs, or individuals performing other roles are operating in compliance with the appropriate CPS or RPS
- Develop, maintain, and approve any RPSs that govern RAs and TAs operating under the CPS

#### *9.6.5.4 Agency POC*

Agency POCs shall do the following:

- Coordinate with the ANMA for the Agency providing CA services to determine roles and responsibilities, including development, approval, and maintenance of an RPS for RAs and TAs operating under this policy, if required
- Ensure that any RA Officers, TAs, or individuals performing other roles are operating in compliance with the appropriate CPS or RPS

## 9.7 DISCLAIMERS OF WARRANTIES

CASs and RAs operating under this CP may not disclaim any responsibilities described in this CP.

## 9.8 LIMITATIONS OF LIABILITY

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

## 9.9 INDEMNITIES

No stipulation.

## 9.10 TERM AND TERMINATION

### 9.10.1 Term

This CP becomes effective when approved by the NSS PKI PMA. It shall remain in effect until either a new NSS PKI CP is approved by the NSS PKI PMA or the NSS PKI is terminated.

### 9.10.2 Termination

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

### 9.10.3 Effect of Termination and Survival

The responsibilities for protecting business confidential and personal information, and for protecting intellectual property rights, shall survive termination of this CP.

Intellectual property rights shall survive this CP in accordance with the Intellectual Property laws of the United States.

The archive requirements of this CP remain in effect through the end of the archive period for the last certificate issued. Other requirements concerning the organization and operations of the NSS PKI infrastructure; certificate application, usage, and revocation; physical and technical security controls; audits; and other business and legal matters shall remain in effect through the expiration date of the last certificate issued and/or cessation of operations and closure of the NSS PKI. See Section 5.8.1 for additional requirements.

## 9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

The NSS PKI PMA shall establish appropriate procedures for communications with CAs cross-certified with this CP.

## 9.12 AMENDMENTS

### 9.12.1 Procedure for Amendment

The NSS PKI Member Governing Body, on behalf of the NSS PKI PMA, shall review this CP at least once every year. Corrections, updates, or changes to this CP shall be made available to CNSS member agencies. Suggested changes to this CP shall be communicated to the contact in Section 1.5.2. All such communication shall include a description of the change, a change justification, and contact information for the person requesting the change.

The NSS PKI Member Governing Body shall review requested changes. Changes approved by the Member Governing Body shall be forwarded to the NSS PKI PMA for final review and acceptance. The NSS PKI PMA shall accept, accept with modifications, or reject any proposed change.

Administrative updates, such as typographical errors, may be approved by the NSS PKI PMA without requiring full review by the NSS PKI Member Governing Body.

### 9.12.2 Notification Mechanism and Period

All policy changes under consideration by the NSS PKI PMA shall be disseminated to CNSS member agencies for a period of at least one month prior to incorporation.

Accepted changes shall be incorporated into an updated, signed CP, which shall be published on the NSS PKI web site in accordance with Section 2.

### 9.12.3 Circumstances under which OID must be Changed

The Certificate Policy OID shall only change if the change in the CP results in a material change to the trust by Relying Parties.

## 9.13 DISPUTE RESOLUTION PROVISIONS

The NSS PKI PMA shall decide any disputes over the interpretation or applicability of the NSS PKI CP. The NSS PKI PMA may facilitate the resolution between entities when conflicts arise as a result of the use of certificates issued under this policy.

## 9.14 GOVERNING LAW

The construction, validity, performance, and effect of certificates issued under this CP for all purposes shall be governed by U.S. Federal law (statute, case law), or regulations, directives or policies.

## 9.15 COMPLIANCE WITH APPLICABLE LAW

All CASs operating under this CP are required to comply with applicable Federal law, regulations, directives, and policies. See Section 9.14.

## 9.16 MISCELLANEOUS PROVISIONS

### 9.16.1 Entire Agreement

No stipulation.

### 9.16.2 Assignment

No stipulation.

### 9.16.3 Severability

Should it be determined that one section of this CP is incorrect or invalid, the other sections shall remain in effect until the CP is updated. The process for updating this CP is described in Section 9.12. Responsibilities, requirements, and privileges of this document are merged to the newer edition upon release of that newer edition.

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

No stipulation.

### 9.16.5 Force Majeure

No stipulation.

## 9.17 OTHER PROVISIONS

No stipulation.

# APPENDIX A REFERENCES

| Number | Title | Date |
|---|---|---|
| 41 CFR 105-60.605 | *41 CFR 105-60.605 - Procedure in the event of a demand for production or disclosure*<br>United States Code | |
| ABA DSG | *Digital Signature Guidelines*<br>American Bar Association<br>http://www.abanet.org/scitech/ec/isc/dsgfree.html | August 1996 |
| CNSS 4005 | *CNSS 4005, Safeguarding COMSEC Facilities and Material*<br>Committee for National Security Systems | August 1997, Amended September 2005 |
| CNSS 4009 | *CNSS 4009, National Information Assurance (IA) Glossary*<br>Committee for National Security Systems<br>www.cnss.gov/Assets/pdf/cnssi_4009.pdf | June 2006 |
| CNSSP 25 | *CNSS Policy (CNSSP) Number 25, National Policy for Public Key Infrastructure in National Security Systems*<br>Committee for National Security Systems | March 2009 |
| FIPS 140 | *Federal Information Processing Standard 140, Security Requirements For Cryptographic Modules*<br>National Institute for Standards and Technology FIPS Publication<br>http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf | May 2001 |
| FIPS 186 | *Federal Information Processing Standard 186, Digital Signature Standard*<br>National Institute for Standards and Technology FIPS Publication<br>http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf | January 2000 |
| FIPS 201 | *Federal Information Processing Standard 201, Personal Identity Verification (PIV) of Federal Employees and Contractors*<br>National Institute for Standards and Technology FIPS Publication<br>http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf | March 2006 |
| FORM I-9 | *OMB No. 1615-004, Form I-9, Employment Eligibility Verification*<br>http://www.uscis.gov/files/form/I-9.pdf | May 2007 |
| FTCA | *Federal Tort Claims Act (FTCA)*<br>United States Code 28 U.S.C. 171 | |
| ITU X.500 | *X.500 : Information technology - Open Systems Interconnection - The Directory: Overview of Concepts, Models and Services*<br>International Telecommunications Union<br>http://www.itu.int/rec/T-REC-X.500-200508-I/en | August 2005 |
| ITU X.509 | *X.509 : Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks*<br>International Telecommunications Union<br>http://www.itu.int/rec/T-REC-X.509-200508-I | August 2005 |
| NSD 42 | *National Security Directive (NSD) 42, National Policy for the Security of National Security Telecommunications and Information System*<br>Presidential Directive | July 1990 |

| Number | Title | Date |
|---|---|---|
| NSS PKI PROF | *CNSS PKI Profiles Specification*<br>Contact the NSS PKI Member Governing Body for copy of most recent version | |
| PRIVACT | *5 U.S.C. 552a, Privacy Act of 1974*<br>United States Code | |
| RFC 2560 | *IETF RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*<br>Internet Engineering Task Force<br>http://www.ietf.org/rfc/rfc2560.txt | June 1999 |
| RFC 3647 | *IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*<br>Internet Engineering Task Force<br>http://www.ietf.org/rfc/rfc3647.txt | November 2003 |
| RFC 5322 | *Internet Engineering Task Force (IETF) RFC 5322 Internet Message Format*<br>Internet Engineering Task Force<br>http://www.ietf.org/rfc/rfc5322.txt | October 2008 |
| SP 800-57 | *NIST Special Publication 800-57, Recommendation for Key Management – Part 1: General*<br>National Institute for Standards and Technology<br>http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf | March 2007 |

# APPENDIX B ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| ANMA | Agency NSS PKI Management Authority |
| AES | Advanced Encryption Standard |
| AIA | Authority Information Access |
| CA | Certification Authority |
| CAS | Certification Authority System |
| CMCS | COMSEC Material Control System |
| CMMI | Capability Maturity Model Integration |
| CNSS | Committee for National Security Systems |
| CNSSP | CNSS Policy |
| CP | Certificate Policy |
| CPS | Certification Practice Statement |
| CRL | Certificate Revocation List |
| CSOR | Computer Security Objects Register |
| CSS | Certificate Status Server |
| dc | Domain Component |
| DIRNSA | Director, National Security Agency |
| DN | Distinguished Name |
| FIPS | Federal Information Processing Standard |
| HTTP | Hyper Text Transfer Protocol |
| IA | International Alphabet |
| ID | Identification |
| IDS | Intrusion Detection System |
| IETF | Internet Engineering Task Force |
| IP | Internet Protocol |
| ITU | International Telecommunications Union |
| KES | Key Escrow System |
| LDAP | Lightweight Directory Access Protocol |
| MOA | Memorandum of Agreement |
| NIST | National Institute for Standards and Technology |
| NSA | National Security Agency |
| NSD | National Security Directive |
| NSS PKI | National Security Systems PKI |
| OCSP | Online Certificate Status Protocol |
| ODNI | Office of the Director of National Intelligence |
| OID | Object Identifier |
| PIN | Personal Identification Number |

| | |
|---|---|
| PIV | Personal Identity Verification |
| PKI | Public Key Infrastructure |
| PMA | Policy Management Authority |
| POC | Point of Contact |
| RA | Registration Authority |
| RPS | Registration Practice Statement |
| SSBI | Single Scope Background Investigation |
| TA | Trusted Agent |
| TLS | Transport Layer Security |
| U.S. | United States |
| UTF | Unicode Transformation Format |

# APPENDIX C GLOSSARY OF TERMS

| Term | Definition |
|---|---|
| Agency NSS PKI Management Authority (ANMA) | The entity within an agency that operates a CA under this policy that is responsible for all aspects of management of the NSS PKI program for that agency, and for participating in the NSS PKI Member Governing Body. |
| Agency NSS PKI Point of Contact (POC) | The entity within an agency that does not operate a CA under this policy but that obtains certificates from a Common Services Provider CA operated under this policy. The POC is responsible for all aspects of management of the NSS PKI program for that agency and is responsible for participating in the NSS PKI Member Governing Body. |
| Agency Repository | A repository maintained by each agency that operates a CA. The repository shall support HTTP or LDAP to provide CA certificates and CRLs and collects information from the central repository for use by systems on that agency's network. |
| 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. [CNSS 4009]; A process used to confirm the identity of a person or to prove the integrity of specific information |
| Bits of Security | See Security Strength |
| Central Repository | A repository that provides CA certificates and CRLs that supports overall NSS PKI operations with both HTTP and LDAP interfaces. The central repository function may consist of one or more repositories to support overall NSS PKI operations at the discretion of the NSS PKI Member Governing Body or the PMA. The central repository shall collect necessary information from the agency repositories. |
| Certificate | A digital representation of information which at least<br>• Identifies the certification authority issuing it<br>• Names or identifies its Subscriber<br>• Contains the Subscriber's public key<br>• Identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABA DSG] |
| Certification Authority (CA) | An entity authorized to create, sign, and issue public key certificates. |
| Certification Authority System (CAS) | The collection of hardware, software, and operating personnel that create, sign, and issue public key certificates to Subscribers. |
| Certificate Policy (CP) | A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range. [RFC 3647] |
| Certificate Policy OID | The certificate policy object identifier (OID) is a numeric string that is used to uniquely identify the set of certificate policy requirements stipulated in a CP. |
| Certificate Revocation List (CRL) | These are digitally signed "blacklists" of revoked certificates. CAs periodically issue CRLs, and users can retrieve them on demand via repositories. |
| Certificate Status Server (CSS) | An authority that provides status information about certificates on behalf of the CA through online transactions (e.g., an Online Certificate Status Protocol (OCSP) responder) |

| Term | Definition |
|---|---|
| Certification Practice Statement (CPS) | A document representing a statement of practices a CA employs in issuing certificates. |
| CNSS | Committee on National Security Systems, a U.S. government organization providing guidance for the security of national security systems. |
| Code Signing Certificate | A certificate issued for the purpose of digitally signing executables and scripts to confirm the software author and guarantee that the code has not been altered or corrupted since it was signed by use of a cryptographic hash. |
| Common Services Provider | A provider of services, typically CA services, to agencies that do not operate their own CA. |
| Confidentiality | Assurance that information is not disclosed to unauthorized entities or processes. [CNSS 4009] |
| Content Signing Certificate | A certificate issued for the purpose of digitally signing information (content) to confirm the author and guarantee that the content has not been altered or corrupted since it was signed by use of a cryptographic hash. |
| Cross Certificate | A certificate issued from a CA that signs the public key of another CA not within its trust hierarchy that establishes a trust relationship between the two CAs. {Note: This is a more narrow definition than described in X.509.} |
| Encryption Certificate | A certificate containing a public key that can encrypt or decrypt electronic messages, files, documents, or data transmissions, or establish or exchange a session key for these same purposes. Key management sometimes refers to the process of storing protecting and escrowing the private component of the key pair associated with the encryption certificate. |
| Identity Certificate | A certificate that provides authentication of the identity claimed. Within the NSS PKI, identity certificates may be used only for authentication or may be used for both authentication and digital signatures. |
| Integrity | Protection against unauthorized modification or destruction of information. [CNSS 4009] |
| Intermediate Certification Authority (CA) | A CA that is signed by a superior CA (e.g., a Root CA or another Intermediate CA) and signs CAs (e.g., another Intermediate or Subordinate CA). The Intermediate CA exists in the middle of a trust chain between the Trust Anchor, or Root, and the subscriber certificate issuing Subordinate CAs. |
| Key Compromise | Disclosure of the private key to unauthorized persons, or a violation of the security policy of the PKI in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of the private key may have occurred. |
| Key Escrow | The retention of the private component of the key pair associated with a Subscriber’s encryption certificate to support key recovery. |
| Key Escrow System (KES) | The system responsible for storing and providing a mechanism for obtaining copies of private keys associated with encryption certificates, which are necessary for the recovery of encrypted data. |
| Key Recovery | The process for obtaining a copy of an escrowed private key from the KES. |
| Legacy NSS PKI | An operational PKI on an agency’s classified network prior to the establishment of the NSS PKI. |
| Modification | The process of creating a new certificate with a new serial number that differs in one or more fields from the old certificate. The new certificate may have the same or different subject public key. |

| Term | Definition |
|---|---|
| Name Subscriber | A Name Subscriber is an individual (i.e., person) whose name appears as the subject in a certificate. The Name subscriber is tightly coupled with the name certificate in which they are named. |
| NSS PKI | A Public Key Infrastructure (PKI) for SECRET-high collateral classified networks. |
| NSS PKI Member Governing Body | The organization established from the participating agencies to assist the PMA and provide governance and oversight to the NSS PKI. |
| PKI Sponsor | A person who is responsible for the private key associated with a certificate and who asserts that the certificate and associated private key are being used in accordance with this CP. |
| Policy Management Authority (PMA) | Individual or 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. |
| Private Key | A mathematical key (kept secret by the holder) used to create digital signatures and, depending upon the algorithm, to decrypt messages or files encrypted (for confidentiality) with the corresponding public key. |
| Public Key | A mathematical key that has public availability and that applications use to verify signatures created with its corresponding private key. Depending on the algorithm, public keys can encrypt messages or files that the corresponding private key can then decrypt. |
| Pubic Key Infrastructure (PKI) | The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. Framework established to issue, maintain, and revoke public key certificates. |
| Registration Authority (RA) | An entity authorized by the CAS to collect, verify, and submit information provided by potential Subscribers which is to be entered into public key certificates. The term RA refers to hardware, software, and individuals that collectively perform this function. |
| Registration Authority (RA) Officer | A trusted role, performed by an individual who is responsible for any of the duties of certificate issuance, certificate revocation, or key recovery. |
| Registration Practice Statement (RPS) | A document representing a statement of practices an RA employs when performing RA duties for a CAS. |
| Re-Key | The process of creating a new certificate with a new validity period, serial number, and public key while retaining all other Subscriber information in the original certificate |
| Relying Party | An entity that relies on the validity of the binding of the Subscriber’s name to a public key to verify or establish the identity and status of an individual, role, or system or device; the integrity of a digitally signed message; the identity of the creator of a message; or confidential communications with the Subscriber |
| Renewal | 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. [ABA DSG] |
| Restoration | The process of changing the status of a suspended (i.e., temporarily invalid) certificate to valid. |
| Revocation | The process of permanently ending the binding between a certificate and the identity asserted in the certificate from a specified time forward. |

| Term | Definition |
|---|---|
| Role Subscriber | A Role Subscriber is a role, group, or organization whose name appears as the subject in a certificate. |
| Root Certificate Authority (CA) | The CA that issues the first certificate in a certification chain. |
| Security Auditor | A trusted role that is responsible for auditing the security of CASs and RAs, including reviewing, maintaining, and archiving audit logs and performing or overseeing internal audits of CASs and RAs. |
| Security Strength | A number associated with the amount of work (that is, the number of operations) that is required to break a cryptographic algorithm or system. In this policy, security strength is specified in bits and is a specific value from the set {80, 112, 128, 192, 256} [SP 800-57] |
| Signature Certificate | A public key certificate that contains a public key intended for verifying digital signatures rather than authenticating, encrypting data, or performing any other cryptographic functions. |
| Subordinate Certificate Authority (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. |
| 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. [ABA DSG]. |
| Suspension | The process of changing the status of a valid certificate to suspended (i.e., temporarily invalid) |
| System or Device Certificate | A System or Device certificate contains a system or device name as the subject. Examples of systems or devices are workstations, guards, firewalls, routers, web server, database server, and other infrastructure components |
| System or Device Subscriber | A System or Device Subscriber is the system or device whose name appears as the subject in a certificate. |
| Technical Non-Repudiation | The contribution public key mechanisms make to the provision of technical evidence supporting a non-repudiation security service. |
| Trusted Agent (TA) | An individual explicitly aligned with one or more RA Officers who has been delegated the authority to perform a portion of the RA functions. A TA does not have privileged access to CAS components to authorize certificate issuance, certificate revocation, or key recovery. |