



X.509 Certificate Policy
for the
Government Printing Office
Certification Authority
(GPO-CA)

July 1, 2006

Version 1.2

FOR OFFICIAL USE ONLY

SIGNATURE PAGE

Chair, Government Printing Office Public Key Infrastructure Steering Committee DATE

Chair, Government Printing Office Public Key Infrastructure Policy Authority DATE

Chief Information Officer, Government Printing Office DATE

TABLE OF CONTENTS

1. INTRODUCTION.....	1
1.1 OVERVIEW	1
1.1.1 Certificate Policy (CP).....	1
1.1.2 GPO CP and CPS Relationship.....	1
1.1.3 External CA Interoperation.....	1
1.1.4 Scope.....	2
1.2 IDENTIFICATION	2
1.3 COMMUNITY AND APPLICABILITY	2
1.3.1 PKI Authorities	2
1.3.2 Related Authorities	4
1.3.3 End Entities.....	4
1.3.4 Applicability	5
1.4 CONTACT DETAILS.....	6
1.4.1 Specification Administration Organization	6
1.4.2 Contact Person	6
1.4.3 Person Determining CPS Suitability for the Policy	6
2. GENERAL PROVISIONS.....	7
2.1 OBLIGATIONS	7
2.1.1 CA Obligations	7
2.1.2 RA Obligations	7
2.1.3 Subscriber Obligations.....	7
2.1.4 Relying Party Obligations.....	7
2.1.5 Repository Obligations	7
2.1.6 Certificate Issuance to Non-GPO Parties.....	8
2.2 LIABILITY	8
2.3 FINANCIAL RESPONSIBILITY	8
2.3.1 Indemnification by Relying Parties and Subscribers	8
2.3.2 Fiduciary Relationships	8
2.3.3 Administrative Processes	9
2.4 INTERPRETATION AND ENFORCEMENT	9
2.4.1 Severability of Provisions, Survival, Merger, and Notice	9
2.4.2 Dispute Resolution Procedures.....	9
2.5 FEES	9
2.6 PUBLICATION AND REPOSITORY.....	9
2.6.1 Publication of CA Information	9
2.6.2 Frequency of Publication	9
2.6.3 Access Controls	9
2.6.4 Repositories.....	10
2.7 COMPLIANCE AUDIT	10
2.7.1 Compliance Audit Frequency	10
2.7.2 Identity/Qualifications of Compliance Auditor	10
2.7.3 Compliance Auditor’s Relationship to Audited Party	10
2.7.4 Topics Covered by Compliance Audit.....	10
2.7.5 Actions Taken as a Result of Deficiency	11

2.7.6	Communication of Result	11
2.8	CONFIDENTIALITY.....	11
2.9	INTELLECTUAL PROPERTY RIGHTS.....	11
3.	IDENTIFICATION AND AUTHENTICATION	12
3.1	INITIAL REGISTRATION.....	12
3.1.1	Types of Names	12
3.1.2	Need for Names to be Meaningful.....	12
3.1.3	Rules for Interpreting Various Name Forms	12
3.1.4	Uniqueness of Names	12
3.1.5	Name Claim Dispute Resolution Procedure	13
3.1.6	Recognition, Authentication and Role of Trademarks	13
3.1.7	Method to Prove Possession of Private Key	13
3.1.8	Authentication of Organization Identity	13
3.1.9	Authentication of Individual Identity.....	13
3.1.10	Authentication of Component Identities.....	14
3.2	CERTIFICATE RENEWAL, UPDATE, AND ROUTINE RE-KEY	15
3.2.1	Certificate Re-key	15
3.2.2	Certificate Renewal.....	15
3.2.3	Certificate Update	15
3.3	OBTAINING A NEW CERTIFICATE AFTER REVOCATION.....	16
3.4	REVOCATION REQUEST	16
4.	OPERATIONAL REQUIREMENTS.....	17
4.1	APPLICATION FOR A CERTIFICATE.....	17
4.1.1	Delivery of Public Key for Certificate Issuance	17
4.2	CERTIFICATE ISSUANCE.....	17
4.2.1	Subscriber's Private Key Delivery	18
4.2.2	GPO-CA Public Key Delivery and Use.....	18
4.3	CERTIFICATE ACCEPTANCE	19
4.4	CERTIFICATE SUSPENSION AND REVOCATION	19
4.4.1	Revocation	19
4.4.2	Suspension	21
4.4.3	Revocation Lists.....	21
4.4.4	On-line Revocation/Status Checking Availability	22
4.4.5	Other Forms of Revocation Advertisements Available	22
4.4.6	Checking Requirements for Other Forms of Revocation Advertisements	22
4.4.7	Special Requirements Related to Key Compromise	22
4.5	SECURITY AUDIT PROCEDURE.....	22
4.5.1	Types of Events Recorded	22
4.5.2	Frequency of Processing Data	26
4.5.3	Retention Period for Security Audit Data.....	26
4.5.4	Protection of Security Audit Data.....	26
4.5.5	Security Audit Data Backup Procedures.....	27
4.5.6	Security Audit Collection System (Internal vs. External)	27
4.5.7	Notification to Event-Causing Subject	27
4.5.8	Vulnerability Assessments.....	27
4.6	RECORDS ARCHIVAL.....	27

4.6.1	Types of Events Archived.....	27
4.6.2	Retention Period for Archive.....	28
4.6.3	Protection of Archive.....	29
4.6.4	Archive Backup Procedures.....	29
4.6.5	Requirements for Time-Stamping of Records.....	29
4.6.6	Archive Collection System (Internal or External).....	29
4.6.7	Procedures to Obtain and Verify Archive Information.....	29
4.7	KEY CHANGEOVER	29
4.8	COMPROMISE AND DISASTER RECOVERY	30
4.8.1	Computing Resources, Software, and/or Data are Corrupted.....	30
4.8.2	GPO-CA Signature Keys are Revoked.....	30
4.8.3	GPO-CA Signature Keys are Compromised.....	30
4.8.4	Secure Facility Impaired After a Natural or Other Disaster.....	30
4.9	CA TERMINATION.....	31
5.	PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS	32
5.1	PHYSICAL CONTROLS FOR THE GPO-CA.....	32
5.1.1	Site Location and Construction.....	32
5.1.2	Physical Access.....	32
5.1.3	Electrical Power.....	33
5.1.4	Water Exposures.....	33
5.1.5	Fire Prevention and Protection.....	33
5.1.6	Media Storage.....	33
5.1.7	Waste Disposal.....	33
5.1.8	Off-Site Backup.....	34
5.2	PROCEDURAL CONTROLS FOR THE GPO-CA.....	34
5.2.1	Trusted Roles.....	34
5.2.2	Separation of Roles.....	36
5.2.3	Number of Persons Required Per Task.....	36
5.2.4	Identification and Authentication for Each Role.....	37
5.3	PERSONNEL CONTROLS	37
5.3.1	Background, Qualifications, Experience, and Security Clearance Requirements.....	37
5.3.2	Background Check Procedures.....	37
5.3.3	Training Requirements.....	37
5.3.4	Retraining Frequency and Requirements.....	37
5.3.5	Job Rotation Frequency and Sequence.....	37
5.3.6	Sanctions for Unauthorized Actions.....	38
5.3.7	Contracting Personnel Requirements.....	38
5.3.8	Documentation Supplied to Personnel.....	38
6.	TECHNICAL SECURITY CONTROLS	39
6.1	KEY PAIR GENERATION AND INSTALLATION.....	39
6.1.1	GPO-PKI and GPO-CA Key Pair Generation.....	39
6.1.2	Private Key Delivery to Subscriber.....	39
6.1.3	Public Key Delivery to Certificate Issuer.....	39
6.1.4	GPO-CA Certificates and Public Key Availability and Delivery to Entity CAs..	39
6.1.5	Key Sizes.....	40
6.1.6	Public Key Parameters Generation.....	40

6.1.7	Parameter Quality Checking	40
6.1.8	Subscriber Key Generation	40
6.1.9	Key Usage Purposes (as Per X.509 v3 Key Usage Field)	40
6.2	PRIVATE KEY PROTECTION.....	41
6.2.1	Standards for Cryptographic Module.....	41
6.2.2	GPO-CA Private Key Multi-Person Control	41
6.2.3	Key Escrow of GPO-CA Private Signature Key	41
6.2.4	Private Key Backup	41
6.2.5	Private Key Archival.....	42
6.2.6	Private Key Entry Into Cryptographic Module.....	42
6.2.7	Method of Activating Private Keys	42
6.2.8	Private Key Deactivation Methods	42
6.2.9	Private Signature Key Destruction Method	42
6.3	GOOD PRACTICES REGARDING KEY-PAIR MANAGEMENT	42
6.3.1	Public Key Archival.....	43
6.3.2	Usage Periods for the Public and Private Keys	43
6.4	ACTIVATION DATA.....	43
6.4.1	Activation Data Generation and Installation.....	43
6.4.2	Activation Data Protection.....	43
6.4.3	Other Aspects of Activation Data	43
6.5	COMPUTER SECURITY CONTROLS.....	44
6.5.1	Specific Computer Security Technical Requirements	44
6.5.2	Computer Security Rating.....	44
6.6	LIFE-CYCLE TECHNICAL CONTROLS.....	44
6.6.1	System Development Controls	44
6.6.2	Security Management Controls.....	45
6.6.3	Life Cycle Security Ratings	45
6.7	NETWORK SECURITY CONTROLS	45
6.8	CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS	46
7.	CERTIFICATE AND CARL/CRL PROFILES	47
7.1	CERTIFICATE PROFILE	47
7.1.1	Version Numbers	47
7.1.2	Certificate Extensions	47
7.1.3	Algorithm Object Identifiers.....	47
7.1.4	Name Forms.....	48
7.1.5	Name Constraints.....	48
7.1.6	Certificate Policy Object Identifier.....	48
7.1.7	Usage of Policy Constraints Extension.....	48
7.1.8	Policy Qualifiers Syntax and Semantics	48
7.1.9	Processing Semantics for the Critical Certificate Policy Extension	48
7.2	CARL/CRL PROFILE	48
7.2.1	Version Numbers	48
7.2.2	CARL and CRL Entry Extensions.....	48
8.	SPECIFICATION ADMINISTRATION	49
8.1	SPECIFICATION CHANGE PROCEDURES	49
8.2	PUBLICATION AND NOTIFICATION POLICIES	49

8.3	CPS APPROVAL PROCEDURES	49
8.4	WAIVERS	49
9.	BIBLIOGRAPHY	50
10.	ACRONYMS AND ABBREVIATIONS	52
11.	GLOSSARY	55

RECORD OF CHANGES

Version	Date	Author(s)	Reason	Description
1.0	8 September 2003	CygnaCom Solutions, Inc	Initial Document	Initial Document
1.0.1	1 October 2004	CygnaCom Solutions, Inc	Minor changes for FBCA CP mapping for FBCA cross certification	Address the four comments from the FBCA CP mapping
1.1	27 February 2006	U.S. Government Printing Office	Changes to comply with Federal PKI Common Policy and PKI Shared Service Provider (SSP) requirements	Changes in various sections to comply with Federal PKI Common Policy and PKI Shared Service Provider (SSP) requirements
1.2	1 July 2006	U.S. Government Printing Office	Changes to comply with AICPAWebTrust for CA audit requirements	Changes in various sections to comply with the AICPA WebTrust for CA audit requirements, as recommended by WebTrust auditor and GPO OIG recommendations.

1. INTRODUCTION

This Certificate Policy (CP) defines the certificate policy for use by the Government Printing Office Certification Authority (GPO-CA) to facilitate interoperability between other PKI Domains and CAs External to the GPO-CA. This policy represents a Medium Assurance Level for public key digital certificates. The word “assurance” used in this CP means how well a Relying Party can be certain of the identity binding between the public key and the individual whose subject name is cited in the certificate. In addition, it also reflects how well the Relying Party can be certain that the individual whose subject name is cited in the certificate is controlling the use of the private key that corresponds to the public key in the certificate, and how securely the system which was used to produce the certificate and (if appropriate) deliver the private key to the subscriber performs its task.

This GPO CP is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 2527, Certificate Policy and Certification Practices Statement Framework.

The terms and provisions of this GPO CP shall be interpreted under and governed by applicable Federal law.

1.1 OVERVIEW

1.1.1 Certificate Policy (CP)

GPO-CA certificates contain a registered certificate policy object identifier (OID), which may be used by a Relying Party to decide whether a certificate is trusted for a particular purpose. The party that registers the OID (in this case, the U.S. Government) also publishes the CP, for examination by Relying Parties. Each certificate issued by the GPO-CA will, in the *policyMappings* extension and in whatever other fashion is determined by the GPO-CA to be necessary for interoperability, reflect what mappings the GPO PKI Policy Authority determines shall exist between the GPO CP and the Entity CP.

1.1.2 GPO CP and CPS Relationship

The GPO CP states what assurance can be placed in a certificate issued by the GPO-CA. The GPO CPS states how the GPO-CA establishes that assurance.

1.1.3 External CA Interoperation

This CP provides for interoperability with Entity CAs (CAs external to the GPO, non-GPO-CAs) through cross certification. Interoperability will be established when directed by the GPO-PA and will require a Memorandum of Agreement (MOA), between the GPO-CA and the Entity CA, and may require changes to this CP to address issues associated with liability and other matters.

1.1.4 Scope

The GPO-CA exists to facilitate trusted electronic business transactions for federal organizations. To facilitate the missions of the organizations, interoperability is offered to non-federal entities. The interoperability information in this CP applies equally to federal organizations and other organizations owning or operating PKI domains. As used in this CP, Entity PKI or Entity CA may refer to an organization's PKI, a PKI provided by a commercial service, or a bridge CA serving a community of interest.

1.2 IDENTIFICATION

The Medium Level of Assurance is defined in subsequent sections of this CP. The GPO Medium Assurance CP has a corresponding Object Identifier (OID), to be asserted in certificates issued by the GPO-CA, which comply with the policy stipulations herein. The OIDs are registered under the id-infosec arc as follows:

id-fpki-common-policy ::= {2 16 840 1 101 3 2 1 3 6}

id-fpki-common-hardware ::= {2 16 840 1 101 3 2 1 3 7}

id-fpki-common-devices ::= {2 16 840 1 101 3 2 1 3 8}

csor-certpolicy ::= {2 16 840 1 101 3 2 1}

id-gpo-policies ::= {csor-certpolicy 17}

id-gpo-medium ::= {id-gpo-policies 1}

1.3 COMMUNITY AND APPLICABILITY

The following are roles relevant to the administration and operation of the GPO-CA.

1.3.1 PKI Authorities

1.3.1.1 GPO PKI Policy Authority

The GPO PKI Policy Authority (PA) is a group of GPO personnel. The GPO-PKI-PA (or GPO-PA) is responsible for:

- The Government Printing Office Certification Authority (GPO-CA) Certificate Policy (CP)
- The GPO-CA Certification Practices Statement (CPS)
- Accepting applications from other PKI Domains desiring to interoperate with the GPO-CA
- Determining the mappings between certificates issued by applicant Entity CAs and the levels of assurance set forth in the GPO-CA-CP (which will include objective and

subjective evaluation of the respective CP contents and any other facts deemed relevant by the GPO-PA)

- After a CA is authorized to interoperate with the GPO-CA, ensuring continued conformance of the Entity PKI Domain with applicable requirements is a condition for allowing continued interoperability with the GPO-CA

The GPO-PA will enter into an MOA with the applicant Entity setting forth the respective responsibilities and obligations of both parties, and the mappings between the certificate levels of assurance contained in this CP and those of the Entity CP. Thus, the term “MOA” as used in this CP shall always refer to the Memorandum of Agreement cited in this paragraph.

1.3.1.2 GPO Operational Authority

The GPO Operational Authority (OA) is the organization that operates the GPO-CA, including issuing GPO-CA certificates when directed by the GPO-PA, posting those certificates, Certificate Authority Revocation Lists (CARLs) and Certificate Revocation Lists (CRLs) into the GPO-CA repository, and ensuring the continued availability of the repository to all users. The GPO-CA Operational Authority includes the following roles: Oversight Administrator, Officer, System Administrator, and Backup Operator, all described in later sections of this CP.

1.3.1.3 GPO Operational Authority Oversight Administrator

The OA Oversight Administrator (OAOA) is the individual within the GPO-OA who has principal responsibility for overseeing the proper operation of the GPO-CA including the GPO-CA repository, and who appoints individuals to the positions of GPO-CA Operational Authority (OA).

1.3.1.4 GPO Operational Authority Officers

These officers are the individuals within the GPO-OA, selected by the GPO-OAOA, who operate the GPO-CA and its repository including executing GPO-PA direction to issue CA certificates to CAs or taking other action to effect interoperability between the GPO-CA and Entity CAs.

1.3.1.5 Entity Certification Authority

An Entity wishing to interoperate with the GPO may apply for interoperation. Interoperation requires a mapping between the Entity CP and the GPO CP must be completed and an MOA must be in place. The Policy Mapping and MOA are put in place to ensure the level of security on the Entity CA is comparable to the GPO-CA and specify any additional requirements.

1.3.1.6 GPO Certification Authority

The GPO-CA is the entity operated by the GPO-OA that is authorized by the GPO-PA to create, sign, and issue public key certificates to Entity CAs. The GPO-CA is responsible for all aspects of the issuance and management of a certificate including:

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

-
- Publication of certificates
 - Revocation of certificates
 - Re-key of GPO-CA signing material
 - Ensuring that all aspects of the GPO-CA services, operations and infrastructure related to certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP

The Principal CA (PCA) is a CA within a PKI that has been designated to interoperate directly with Entity CAs, and which issues, either end-entity certificates, cross-certificates, or other means of interoperation. Additionally, this CP may refer to CAs that are “subordinate” to the PCA. The use of this term shall encompass any CA under the control of the PCA that has a certificate issued to it by the PCA or any CA subordinate to the PCA, whether or not a hierarchical or other PKI architecture is used.

1.3.1.7 GPO Registration Authority

The GPO Registration Authority (RA) is the entity that collects and verifies each End Entity’s identity and information to be entered into his or her public key certificate. The GPO-RA performs its function in accordance with the GPO CPS approved by the GPO-PA. The requirements for GPO-RAs are set forth in the sections below.

1.3.1.8 GPO Naming Authority

The GPO Naming Authority is the entity that is responsible for managing the GPO name space.

1.3.2 Related Authorities

CAs operating under this CP will require the services of other security, community, and application authorities, such as compliance auditors and attribute authorities. The GPO CPS shall identify the parties responsible for providing such services, and the mechanisms used to support these services.

1.3.3 End Entities

1.3.3.1 Subscribers

A Subscriber is the entity whose name appears as the subject in a certificate, who asserts that it uses its key and certificate in accordance with the CP asserted in the certificate, and who does not issue certificates. Subscribers include all organizational personnel and, when determined by the GPO-PA, other individuals and possibly certain network or hardware devices such as firewalls and routers when needed for infrastructure protection. CAs are sometimes technically considered “subscribers” in a PKI. However, the term “Subscriber” as used in this document refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information.

1.3.3.2 Relying Parties

A Relying Party is the entity that relies on the validity of the binding of the Subscriber's name to a public key. The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. The Relying Party can use the certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate. A Relying Party may use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use.

1.3.4 Applicability

The sensitivity of the information processed or protected using certificates issued by GPO-CA will vary significantly. Organizations must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. This evaluation is done by each Organization for each application and is not controlled by this CP. This CP specifies security requirements for the Medium Assurance Level. The GPO-CA is intended to support applications involving unclassified information, which can include sensitive unclassified data protected pursuant to Federal statutes and regulations.

The Medium Assurance Level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial.

1.3.4.1 Usage Determination

The Relying Party must first determine the level of assurance required for an application, and if the certificates issued under this CP are appropriate for meeting the needs of that application. This will be determined by evaluating various risk factors including the value of the information, the threat environment, and the existing protection of the information environment. These determinations are made by the Relying Party and are not controlled by the GPO-PA or the GPO-OA. Nonetheless, this CP contains some helpful guidance, set forth below, which Relying Parties may consider in making their decisions. Further, Relying Parties should review more detailed guidance governing the use of electronic signatures (which include the use of digital certificates) issued by the Office of Management and Budget implementing the Government Paperwork Elimination Act (Federal Register May 2000: Volume 65, Number 85, Page 25508), as well as more detailed subordinate guidance issued by other agencies pursuant to OMB direction (such as NIST Special Publication 800-25 covering the technical elements of using digital signatures, and electronic record retention guidance such as that provided by the National Archives and Records Administration).

1.4 CONTACT DETAILS

1.4.1 Specification Administration Organization

The GPO-PA is responsible for all aspects of this CP.

1.4.2 Contact Person

Questions regarding this CP shall be directed to the Chair of the GPO-PA, whose address can be found at <http://www.gpoaccess.gov/pki>

1.4.3 Person Determining CPS Suitability for the Policy

The GPO-PA shall approve the GPO CPS. The GPO-PA is responsible for determining whether the GPO CPS conforms to the GPO CP, and in particular, properly adheres to any policy mappings approved by the GPO-PA between the GPO CP and the Entity CP.

2. GENERAL PROVISIONS

2.1 OBLIGATIONS

The obligations described below pertain to the GPO-CA and Entity CAs.

2.1.1 CA Obligations

The GPO-CA who issues certificates that assert this policy shall comply with the stipulations of this CP and comply with the requirements set forth in the MOA. The GPO-CA shall make GPO certificates and CRL's available in a repository for subscribers, PKI administrators and Relying Parties use.

2.1.2 RA Obligations

The RA who performs registration functions in support of the GPO-CA described in 2.1.1 shall also comply with the GPO CP and CPS, as well as the MOA.

2.1.3 Subscriber Obligations

Subscribers who receive certificates from the GPO-CA shall also be required to comply with the GPO CP and CPS, as well as any applicable requirements in the MOA.

2.1.4 Relying Party Obligations

The GPO CP does not specify what steps a Relying Party should take to determine whether to rely upon a certificate. The Relying Party decides, pursuant to its own policies, what steps to take. The GPO-CA merely provides the tools needed to perform the trust path creation, validation, and certificate policy mappings which the Relying Party may wish to employ in its determination. The GPO-CA shall make GPO certificates and CRL's available in a repository so that Relying Parties may obtain GPO certificates and CRL's for Relying Party use (pursuant to Relying Party policies).

2.1.5 Repository Obligations

The GPO-CA may use a variety of mechanisms for posting information into a repository as required by this CP. These mechanisms at a minimum shall include:

- X.500 Directory Server System that is also accessible through the Lightweight Directory Access Protocol (LDAP)
- Availability of the information as required by the certificate information posting and retrieval stipulations of this CP
- Access control mechanisms when needed to protect repository information as described in later sections

2.1.6 Certificate Issuance to Non-GPO Parties

The GPO-CA may issue certificates to customers, contractors and commercial vendors, for the convenience of the GPO when those parties have a bona fide need to possess a certificate issued by the GPO-CA, as established by the GPO-PA. In each such case, a Subscriber Agreement or similar instrument will be executed, and will contain whatever provisions are determined appropriate by the GPO-PA. Such provisions will address the issues delineated below. All subscribers will be registered as described below in Section 3.1.9, Authentication of Individual Identity.

2.2 LIABILITY

The Government Printing Office disclaims any liability that may arise from use of any certificate issued by the GPO-CA, or the GPO-PA's determination to revoke a certificate issued by the GPO-CA. In no event will the GPO be liable for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to any certificate issued by the GPO-CA.

Certificates are issued and revoked at the sole discretion of the GPO-PA. When the GPO-CA issues a cross-certificate, it does so for the convenience of the GPO. Any review by the GPO of a Entity's CP is for the use of the GPO-CA in determining whether or not interoperability is possible, and if possible, to what extent the Entity's CP maps to the GPO CP. The Entity must determine whether the GPO CP meets its legal and policy requirements. Review of an Entity's CP by the GPO is not a substitute for due care and mapping of CP by the Entity.

2.3 FINANCIAL RESPONSIBILITY

Organizations that are acting as Relying Parties, shall determine what financial limits, if any, they wish to impose for certificates used to consummate a transaction. Acceptance of Medium Assurance Level certificates is entirely at the discretion of the organization acting as a Relying Party and is likely to depend upon several factors such as, the likelihood of fraud, other procedural controls, organization-specific policy, or statutorily imposed constraints.

2.3.1 Indemnification by Relying Parties and Subscribers

No stipulation.

2.3.2 Fiduciary Relationships

No stipulation.

2.3.3 Administrative Processes

Administrative processes pertaining to this CP shall be determined by the GPO-OA pursuant to the agreement between it and the GPO-PA for the operation of the GPO-CA.

2.4 INTERPRETATION AND ENFORCEMENT

2.4.1 Severability of Provisions, Survival, Merger, and Notice

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 8.1

2.4.2 Dispute Resolution Procedures

The GPO-PA shall resolve any disputes associated with the use of the GPO-CA or certificates issued by the GPO-CA.

2.5 FEES

GPO reserves the right to charge fees for any or all PKI related services it may offer or provide.

2.6 PUBLICATION AND REPOSITORY

2.6.1 Publication of CA Information

The GPO-CA shall publish information concerning the GPO-CA necessary to support its use and operation.

2.6.2 Frequency of Publication

Certificates are published as specified in this CP. Certificate status information is published as specified in this CP.

2.6.3 Access Controls

The GPO-CA shall protect any repository information not intended for public dissemination or modification. Public keys and certificate status information in the GPO-CA repository shall be publicly available through the Internet. Access to information in CA repositories shall be determined by the GPO pursuant to its authorizing and controlling statutes.

2.6.4 Repositories

See Section 2.1.5. The publication of data to the repositories will be appropriate to the certificate using community, and in accordance with the local security requirements. This includes information about certificate owners and organizations policies in addition to the directories containing the certificates and CRLs. Publication of certificates to the directories will constitute notification to all subscribers of the issuance of certificates. To facilitate the widest use of certificates, GPO may use an X.500 Directory System in addition to other repositories as deemed appropriate. The GPO CPS shall specify the location and contents of the repositories.

2.7 COMPLIANCE AUDIT

CAs shall have a compliance audit mechanism in place to ensure that the requirements of the GPO CP and CPS are being implemented and enforced.

2.7.1 Compliance Audit Frequency

The GPO CAs and RAs shall be subject to a periodic compliance audit which is no less frequent than once per year.

The GPO-CA has the right to require periodic and aperiodic compliance audits or inspections of CA or RA operations to validate that the entities are operating in accordance with the security practices and procedures described in their respective CPS. Further, the GPO-PA has the right to require aperiodic compliance audits of CAs. The GPO-PA shall state the reason for any aperiodic compliance audit.

2.7.2 Identity/Qualifications of Compliance Auditor

The auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with requirements that the GPO-PA imposes on the issuance and management of GPO-CA certificates. The GPO-OA shall identify the compliance auditor for the GPO-CA. The compliance auditor must perform such compliance audits as a primary responsibility.

2.7.3 Compliance Auditor's Relationship to Audited Party

The compliance auditor for the GPO-CA either shall be a private firm that is independent from the entity being audited, or it shall be sufficiently organizationally separated from that entity to provide an unbiased, independent evaluation. The GPO-PA shall determine whether a compliance auditor meets this requirement.

2.7.4 Topics Covered by Compliance Audit

The purpose of a compliance audit shall be to verify that the GPO-CA subject to this CP, and/or any MOA, is complying with the requirements of those documents.

2.7.5 Actions Taken as a Result of Deficiency

The GPO-PA may determine that the GPO-CA or Entity CA is not complying with its obligations set forth in this CP or the respective MOA. When such a determination is made, the GPO-PA may suspend operation of the GPO-CA, or may direct the GPO-OA to cease interoperating with the affected CA (e.g., by revoking the certificate that the GPO-CA had issued to the affected CA), or may direct that other corrective actions be taken which allow interoperation to continue.

When the compliance auditor finds a discrepancy between how the GPO-CA or Entity CA is designed or is being operated or maintained, and the requirements of this CP, the Entity CP, CPS or the MOA, the following actions shall be performed:

- The compliance auditor shall note the discrepancy
- The compliance auditor shall notify the Entity of the discrepancy. The Entity shall notify the GPO-PA promptly
- The party responsible for correcting the discrepancy shall determine what further notifications or actions are necessary pursuant to the requirements of this CP and the MOA, and then proceed to make such notifications and take such actions without delay.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the GPO-PA may decide to halt temporarily operation of the GPO-CA, to revoke a certificate issued by the GPO-CA, or take other actions it deems appropriate. Procedures for making and implementing such determinations will be developed by the GPO-PA.

2.7.6 Communication of Result

An Audit Compliance Report, including identification of corrective measures taken or being taken by the Entity or GPO-CA, shall be provided to the GPO-PA as set forth in this CP or the CPS. Additionally, where necessary, the results shall be communicated as set forth in this CP or the CPS.

2.8 CONFIDENTIALITY

GPO-CA information not requiring protection shall be made publicly available. Specification of information requiring protection may be defined in an MOA or the CPS.

2.9 INTELLECTUAL PROPERTY RIGHTS

The U.S. Government retains exclusive rights to any products or information developed under or pursuant to this CP.

3. IDENTIFICATION AND AUTHENTICATION

3.1 INITIAL REGISTRATION

3.1.1 Types of Names

The GPO-CA asserting this CP (and when required the Entity CA) shall generate, sign and process certificates that contain an X.500 Distinguished Name (DN). Domain Component elements may be used in addition to the DN. Where DNs are required, subscribers shall have them assigned through their organizations, in accordance with a naming authority. If an X.500 Alternative Subject Name is used it must be marked non-critical.

3.1.2 Need for Names to be Meaningful

The identity certificates issued pursuant to this CP are meaningful only if the names that appear in the certificates can be understood and used by Relying Parties. Names used in the certificates must identify the person or object to which they are assigned in a meaningful way.

When DNs are used, it is preferable that the common name represents the subscriber in a way that is easily understandable for humans. For people, this will typically be a legal name. For equipment, this may be a model name and serial number, or an application process (e.g., Organization X Mail List or Organization Y Multifunction Interpreter).

The GPO-CA shall use DNs in certificates it issues. In the case where a root CA certifies a subordinate CA, the GPO-CA must impose restrictions on the name space authorized in the subordinate CA, which are at least as restrictive as its own name constraints.

Cross certificates issued by the GPO-CA at the Medium Assurance level shall have name constraints excluding the GPO name space (i.e. certificates issued by non-GPO CAs under the GPO name space are not trusted) specified by the GPO Naming Authority.

3.1.3 Rules for Interpreting Various Name Forms

Rules for interpreting name forms shall be contained in the applicable certificate profile and are established by the GPO-PA.

3.1.4 Uniqueness of Names

Name uniqueness across the GPO-CA must be enforced. The GPO CAs and RAs shall enforce name uniqueness within the X.500 name space which they have been authorized. When other name forms are used, they too must be allocated such that name uniqueness across the GPO-CA is ensured.

The GPO shall document in its CPS:

- What name forms shall be used
- How the CAs and RAs will allocate names within the Subscriber community to guarantee name uniqueness among current and past Subscribers

3.1.5 Name Claim Dispute Resolution Procedure

The GPO-PA shall resolve any name collisions brought to its attention that may affect interoperability using the GPO-CA.

3.1.6 Recognition, Authentication and Role of Trademarks

No stipulation.

3.1.7 Method to Prove Possession of Private Key

In all cases where the party named in a certificate generates its own keys, then that party shall be required to prove possession of the private key that corresponds to the public key in the certificate request. For signature keys, this may be done by the entity using its private key to sign a value and providing that value to the GPO-CA. The GPO-CA or Entity CA shall then validate the signature using the party's public key. The GPO-PA may allow other mechanisms that are at least as secure as those cited here.

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

When keyed hardware tokens are delivered to certificate subjects, the delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct subjects. The GPO must maintain a record of validation for receipt of the token by the subject. When any mechanism that includes a shared secret is used, the mechanism shall ensure that the applicant and the GPO-CA are the only recipients of this shared secret.

3.1.8 Authentication of Organization Identity

Requests for GPO-CA certificates in the name of an organization shall include the organization name, address, and documentation of the existence of the organization. The GPO-OA or GPO-RA shall verify the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the organization.

3.1.9 Authentication of Individual Identity

For Subscribers, the GPO-CA shall ensure that the applicant's identity information is verified and checked in accordance with the GPO CP and CPS. The GPO-CA and/or GPO-RA shall ensure that the applicant's identity information and public key are properly bound. Additionally, the GPO-CA and/or GPO-RA shall record the process that was followed for issuance of each

certificate. The process documentation and authentication requirements shall include the following:

- The identity of the person performing the identification
- A signed declaration by that person that he or she verified the identity of the Subscriber as required by the applicable certificate policy
- A unique identifying number from the ID of the verifier and, if in-person identity proofing is done, from the ID of the applicant
- The date and time of the verification
- A declaration of identity signed by the applicant using a handwritten signature. If in-person identity proofing is done, this shall be performed in the presence of the person performing the identity authentication

Identity for all human subscribers is established by in-person appearance before the Registration Authority, Trusted Agent or an entity certified by a State or Federal Agency as being authorized to confirm identities (such as notaries public) who uses a stamp, seal or other mechanism to authenticate their identity confirmation; information provided shall be checked to ensure legitimacy.

Credentials required are either one Federal Government-issued Picture I.D., or two Non-Federal Government I.D.s, one of which shall be a photo I.D.

If an Applicant is unable to perform face-to-face registration alone (e.g., a network device), the applicant shall be represented by a trusted person already issued a digital certificate by the GPO-CA. The trusted person will present information sufficient for registration of the certificate being requested, for both himself/herself and the applicant who the trusted person is representing.

3.1.10 Authentication of Component Identities

Some computing and communications components (routers, firewalls, servers, etc.) will be named as certificate subjects. In such cases, the component must have a human sponsor. The Sponsor is responsible for providing the following registration information:

- Equipment identification or service name
- Equipment public keys
- Equipment authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the CA or RA to communicate with the sponsor when required

The registration information shall be verified to an assurance level commensurate with the certificate assurance level being requested. Acceptable methods for performing this authentication and integrity checking include, but are not limited to:

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

3.2 CERTIFICATE RENEWAL, UPDATE, AND ROUTINE RE-KEY

3.2.1 Certificate Re-key

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a Subscriber periodically obtains new keys and re-establishes its identity. Re-keying a certificate means that a new certificate is created that has the same characteristics and level as the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key) and a different serial number, and it may be assigned a different validity period.

New certificates will need to be issued to Entity CAs by the GPO-CA when the GPO-CA re-keys. Upon re-key of this component, the GPO-CA shall identify and authenticate subscriber either by:

- (a) Performing the initial registration identification process defined in Section 3.1, or
- (b) If it has been less than three years since an Entity CA was identified as required in Section 3.1, using the currently valid certificate issued to the subscriber by the GPO-CA.

Subscribers of the GPO-CA shall identify themselves for the purpose of re-keying. The identity may be established through use of current signature key, except that identity shall be established through initial registration process at least once every six (6) years from the time of initial registration.

3.2.2 Certificate Renewal

Renewing a certificate means creating a new certificate with the same name, key, and other information as the old one, but a new, extended validity period and a new serial number. Certificates may be renewed in order to reduce the size of CRLs. A certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the Subscriber name and attributes are unchanged. Thus, a CA may choose to create a certificate good for one year, renew it twice (each for a one-year period), and then re-key at the end of the third year.

3.2.3 Certificate Update

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

For example, GPO-CA may choose to update a certificate of a Subscriber whose characteristics have changed (e.g., has just received a medical degree). The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or updated.

Further, if an individual's name changes (e.g., due to marriage), then proof of the name change must be provided to the RA or other designated agent in order for an updated certificate having the new name to be issued.

Finally, when a CA updates its private signature key and thus generates a new public key, the CA shall notify all CAs, RAs, and subscribers that rely on the CA's certificate that it has been changed. For self-signed ("root") certificates, such certificates shall be conveyed to users in a secure fashion to preclude malicious substitution attacks.

3.3 OBTAINING A NEW CERTIFICATE AFTER REVOCATION

In the event of certificate revocation due to loss, compromise, suspected compromise, or return to employment, issuance of a new certificate shall always require that the party go through the initial registration process per Section 3.1 above.

3.4 REVOCATION REQUEST

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

4. OPERATIONAL REQUIREMENTS

4.1 APPLICATION FOR A CERTIFICATE

The following steps are required of a subscriber when applying for a GPO certificate:

- Establish need for certificate
- Establish identity of subscriber
- Obtain public and private key pairs for each certificate required
- Prove to the RA or CA that the Public key forms a functioning key pair with the private key that is held by the subscriber
- Provide a point of contact for verification of any roles or authorizations requested

CAs asserting to this CP shall certify Entity CAs (to include cross certification) only as authorized by the GPO-PA.

4.1.1 Delivery of Public Key for Certificate Issuance

Public keys must be delivered for certificate issuance in a way that binds the applicant verified identification to the public key. This binding may be accomplished using cryptography. If cryptography is used, it must be at least as strong as that employed in certificate issuance. Additionally this binding may also be accomplished using non-cryptographic physical and procedural mechanisms. These mechanisms may include, but are not limited to, floppy disk (or other storage medium) sent via registered mail or courier, or by delivery of a token to a certificate issuer for local key generation at the point of certificate issuance or request. The method used for public key delivery shall be defined in the GPO CPS.

In those cases where public/private key pairs are generated by the GPO-CA on behalf of the Subscriber, the GPO-CA shall implement secure mechanisms to ensure that the token on which the public/private key pair is held is securely sent to the proper Subscriber. The GPO-CA shall also implement procedures to ensure that the token is not activated by an unauthorized entity.

4.2 CERTIFICATE ISSUANCE

Upon receiving a request for a certificate, the GPO CA or RA shall respond in accordance with the requirements set forth in the GPO CP and CPS.

The certificate request may contain an already built ("to-be-signed") certificate. This certificate will not be signed until the process set forth in the GPO CP and CPS has been met.

While the Subscriber may do most of the data entry, it is still the responsibility of the RA to verify that the information is correct and accurate. This may be accomplished through a system

approach linking trusted databases containing personnel information, or other equivalent authenticated mechanisms, or through personal contact with the Subscriber's sponsoring organization. If databases are used to confirm Subscriber information, then these databases must be protected from unauthorized modification to a level commensurate with the level of assurance of the certificate being sought.

To the extent practical, certificates once created shall be checked to ensure that all fields and extensions are properly populated. This may be done through software that scans the fields and extensions looking for any evidence that a certificate was improperly manufactured.

4.2.1 Subscriber's Private Key Delivery

A private key will be generated and remain within the cryptographic boundary of the cryptographic module. If the owner of the module generates the key, then there is no need to deliver the private key. If the key is generated elsewhere, then the module must be delivered to the Subscriber. Accountability for the location and state of the module must be maintained until the Subscriber accepts possession of it. The Subscriber shall acknowledge receipt of the module. Under no circumstances shall anyone other than the Subscriber have knowledge of or control over private signing keys. Anyone who generates a private signing key for a Subscriber shall not retain any copy of the key. Hardware tokens containing GPO-CA private signature keys may be backed-up in accordance with security audit requirements defined in this CP and the GPO CPS.

Normally, a certificate shall be issued to a single Subscriber. For cases where there are several entities acting in one capacity, and where non-repudiation for transactions is not desired, a certificate may be issued that corresponds to a private key that is shared by multiple Subscribers. In these cases:

- An Information Systems Security Office or equivalent shall be responsible for ensuring control of the private key, including maintaining a list of Subscribers who have access to use of the private key, and accounting for which Subscriber had control of the key at what time
- The list of those holding the shared private key must be provided to, and retained by the GPO-CA
- The procedures for issuing tokens for use in shared key applications must comply with all other stipulations of this CP (e.g., key generation, private key protection, and Subscriber obligations)

4.2.2 GPO-CA Public Key Delivery and Use

The public key of the GPO-CA must be available for certification trust paths to be created and verified. To extract the key from that certificate with confidence that it has not been altered, the GPO-CA must ensure that its users have its self-signed root certificate in a trustworthy fashion. Such a self-signed root certificate is sometimes called a Trusted Certificate. Acceptable methods for Trusted Certificate delivery include but are not limited to:

- The GPO-CA loading a Trusted Certificate onto tokens delivered to Relying Parties via secure mechanisms

-
- Secure distribution of Trusted Certificates through secure out-of-band mechanisms
 - Comparison of certificate hashes or fingerprints against Trusted Certificate hashes or fingerprints made available via authenticated out-of-band sources (note that fingerprints or hashes posted in-band along with the certificate are not acceptable as an authentication mechanism)
 - Loading certificates from web sites secured with a currently valid certificate of equal or greater assurance level than the certificate being downloaded

4.3 CERTIFICATE ACCEPTANCE

A Subscriber shall be required to sign, using a handwritten signature, a document containing the requirements the Subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate. The document shall contain the following requirements at a minimum:

- The Subscriber shall accurately represent themselves in all communications with the PKI authorities and other Subscribers.
- The Subscriber shall notify, in a timely manner, the CA that issued their certificates of suspicion that their private keys are compromised or lost, in the event that occurs.

4.4 CERTIFICATE SUSPENSION AND REVOCATION

4.4.1 Revocation

4.4.1.1 Circumstances for Revocation of a Certificate Issued by the GPO-CA

A certificate shall be revoked when the binding between the subject and the subject's public key contained within a certificate is no longer considered valid. Examples of circumstances that invalidate the binding include:

- Identifying information in the certificate has become invalid
- The Subscriber or CA can be shown to have violated, or is suspected of violating, the requirements of the GPO CP, or MOA
- The private key has been or is suspected of having been compromised, or has been lost, stolen, or destroyed in a fashion where there is potential for compromise or loss of control over the use of the private key

Additionally, a Subscriber may always request the revocation of his or her certificate directly. Whenever any of the above circumstances occur, the associated certificate shall be revoked and

placed on the CRL. Revoked certificates shall be included on all new publications of the certificate status information at least until the certificates expire.

4.4.1.2 Who can Request Revocation of a Certificate Issued by the GPO-CA

A GPO-CA issued certificate may be revoked at the direction of the GPO-PA, or an authenticated request by the RA, subscriber, or a designated official. (the designated official shall be identified and authorized in the GPO CP, CPS, or MOA to make such a request).

The process for requesting revocation of a Subscriber certificate issued by the GPO-CA shall be set forth in the GPO CP or CPS. Revocation normally will proceed once:

- The GPO-CA receives sufficient evidence of compromise or loss of the subscriber's corresponding private key
- An authenticated request is made to the GPO-CA by the holder of the private key
- Someone in his or her supervisory chain, or an officially designated administrative or information security officer, makes an authenticated request for revocation

4.4.1.3 Procedure for Revocation Request

A request to revoke a certificate 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). Only the GPO-PA may direct the GPO-OA to revoke certificates issued by the GPO-CA.

Authentication of certificate revocation requests is important to prevent malicious revocation of certificates by unauthorized parties. In particular, if the revocation is being requested for reason of key compromise or suspected fraudulent use, then the Subscriber's or the RA's revocation request must so indicate. If a RA performs this on behalf of a Subscriber, a formal, signed message format known to the CA shall be employed. All requests shall be authenticated; for signed requests from the certificate subject, or from an RA, verification of the signature is sufficient.

Upon receipt of a revocation request involving a GPO-PCA issued certificate, the GPO-OA shall authenticate the request and apprise the GPO-PA. The GPO-PA may, at its discretion, take whatever measures it deems appropriate to verify the need for revocation. If the revocation request appears to be valid, the GPO-PA shall direct the GPO-CA to revoke the certificate by placing its serial number and other identifying information on a CARL/CRL and then post the CARL/CRL in the GPO-CA repository, in addition to any other revocation mechanisms used. The GPO-PA at its discretion may set forth emergency procedures for the GPO-CA to use to effect immediate revocation of a certificate issued by the GPO-CA when appropriate.

For PKI implementations using hardware tokens, a Subscriber ceasing its relationship with an organization that sponsored the certificate shall, prior to departure, surrender to the organization (through any accountable mechanism) all cryptographic hardware tokens that were issued by or on behalf of the sponsoring organization. If a Subscriber leaves an organization all the Subscriber's certificates shall be immediately revoked. The token shall be zeroized or destroyed upon, surrender and shall be protected from malicious use between surrender and zeroization or destruction.

4.4.1.4 Certificate Revocation

Revocation shall take effect upon the publication of status information (identifying the reason for the revocation, which may include loss, compromise, or termination of employment) within the time limits as specified in Section 4.4.3.1 (starting from the time the request is authenticated or sufficient evidence of compromise or loss is received). Information about a revoked certificate shall remain in the status information at least until the certificate expires. A certificate *may* be removed from CRLs issued after the revoked certificate expires.

4.4.1.5 Revocation Request Grace Period

The GPO-CA shall revoke certificates upon request as quickly as is practical.

4.4.2 Suspension

Suspension shall not be used by the GPO-CA.

4.4.3 Revocation Lists

All GPO-CAs shall issue Certificate Authority Revocation Lists (CARLs) and Certificate Revocation Lists (CRLs). To the extent practical, the contents of CARLs and CRLs shall be checked before issuance to ensure that all information is correct. This may be done using software that scans the CARLs and CRLs looking for any evidence of an improperly manufactured CARL or CRL.

4.4.3.1 Revocation Lists Issuance Frequency

CRLs shall be issued in accordance with the following frequency requirements:

- CAs that only issue certificates to CAs and that operate offline must issue CRLs at least once every 24 hours, and the *nextUpdate* time in the CRL may be no later than 24 hours after issuance time.
- CAs that issue certificates to subscribers or operate online must issue CRLs at least once every 18 hours, and the *nextUpdate* time in the CRL may be no later than 18 hours after issuance time.

Certificate status information may be issued more frequently than the issuance frequency described above. CRLs shall be issued within 18 hours of notification of loss or compromise of private key. The GPO-CA shall ensure that superseded certificate status information is removed from the repository upon posting of the latest certificate status information.

Certificate status information shall be published not later than the next scheduled update. This will facilitate the local caching of certificate status information for off-line or remote (laptop) operation. The GPO shall coordinate with the repositories to which they post certificate status information to reduce latency between creation and availability. Superseded certificate status information shall be removed from the repository system upon posting of the latest certificate status information.

4.4.3.2 CARL/CRL Checking Requirements

Use of revoked certificates could have damaging or catastrophic consequences. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party, considering the risk, responsibility, and consequences for using a certificate whose revocation status cannot be guaranteed.

4.4.4 On-line Revocation/Status Checking Availability

In addition to CARL/CRLs, Entity CAs and Relying Party client software may optionally support on-line status checking. Client software using on-line status checking need not obtain or process CARL/CRLs. The GPO-PA will determine when and under what circumstances the GPO-CA will provide on-line status checking of GPO-CA certificates.

4.4.5 Other Forms of Revocation Advertisements Available

No stipulation.

4.4.6 Checking Requirements for Other Forms of Revocation Advertisements

No stipulation.

4.4.7 Special Requirements Related to Key Compromise

In the event of a GPO-CA private key compromise or loss, the GPO-CA shall publish a CARL as soon as practical.

4.5 SECURITY AUDIT PROCEDURE

Audit log files shall be generated for all events relating to the security of the GPO-CA. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with *Retention Period for Archive*, Section 4.6.2.

4.5.1 Types of Events Recorded

All security auditing capabilities of the GPO-CA operating system and PKI CA applications required by this CP shall be enabled. As a result, most of the events identified in the table shall be automatically recorded. (Note: the table below may be replaced in future releases of this CP with a reference to the Certificate Issuing and Management Components Protection Profile being developed by NIST.) At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- Type of event

- Date and time the event occurred
- Success or failure indicator when executing the GPO-CA signing process
- Success or failure indicator when performing certificate revocation
- Identity of the entity and/or operator (of the GPO-CA) that caused the event
- Message from any source requesting an action by the GPO-CA is an auditable event (message must include message date and time, source, destination and contents)

Auditable Event
SECURITY AUDIT
Any changes to the Audit parameters, e.g., audit frequency, type of event audited
Any attempt to delete or modify the Audit logs
IDENTIFICATION AND AUTHENTICATION
Successful and unsuccessful attempts to assume a role
Change in the value of maximum authentication attempts
Maximum number of unsuccessful authentication attempts during user login
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
An Administrator changes the type of authenticator, e.g., from password to biometrics
KEY GENERATION
Whenever the GPO-CA generates a key. (Not mandatory for single session or one-time use symmetric keys)
PRIVATE KEY LOAD AND STORAGE
The loading of Component private keys
All access to certificate subject private keys retained within the GPO-CA for key recovery purposes
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE
All 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

Auditable Event
All certificate requests
CERTIFICATE REVOCATION
All certificate revocation requests
CERTIFICATE STATUS CHANGE APPROVAL
The approval or rejection of a certificate status change request
GPO-CA CONFIGURATION
Any security-relevant changes to the configuration of the GPO-CA
ACCOUNT ADMINISTRATION
Roles and users are added or deleted
The access control privileges of a user account or a role are modified
CERTIFICATE PROFILE MANAGEMENT
All changes to the certificate profile
REVOCATION PROFILE MANAGEMENT
All changes to the revocation profile
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT
All changes to the certificate revocation list profile
MISCELLANEOUS
<i>Installation of the Operating System</i>
<i>Installation of the GPO-CA</i>
<i>Installing hardware cryptographic modules</i>
<i>Removing hardware cryptographic modules</i>
<i>Destruction of cryptographic modules</i>
<i>System Startup</i>
<i>Logon Attempts to GPO-CA Apps</i>
<i>Receipt of Hardware / Software</i>
<i>Attempts to set passwords</i>
<i>Attempts to modify passwords</i>

Auditable Event
<i>Backing up GPO-CA internal database</i>
<i>Restoring GPO-CA internal database</i>
<i>File manipulation (e.g., creation, renaming, moving)</i>
<i>Posting of any material to a repository</i>
<i>Access to GPO-CA internal database</i>
<i>All certificate compromise notification requests</i>
<i>Loading tokens with certificates</i>
<i>Shipment of Tokens</i>
<i>Zeroizing tokens</i>
<i>Rekey of the GPO-CA</i>
<i>Configuration changes to the CA server involving:</i>
<i>Hardware</i>
<i>Software</i>
<i>Operating System</i>
<i>Patches</i>
<i>Security Profiles</i>
PHYSICAL ACCESS / SITE SECURITY
<i>Personnel Access to room housing GPO-CA</i>
<i>Access to the GPO-CA server</i>
<i>Known or suspected violations of physical security</i>
ANOMALIES
<i>Software Error conditions</i>
<i>Software check integrity failures</i>
<i>Receipt of improper messages</i>
<i>Misrouted messages</i>
<i>Network attacks (suspected or confirmed)</i>
<i>Equipment failure</i>
<i>Electrical power outages</i>
<i>Uninterruptible Power Supply (UPS) failure</i>

Auditable Event
<i>Obvious and significant network service or access failures</i>
<i>Violations of Certificate Policy</i>
<i>Violations of Certification Practice Statement</i>
<i>Resetting Operating System clock</i>

4.5.2 Frequency of Processing Data

Audit logs shall be reviewed at least once every week. All significant events shall be explained in an audit log summary. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews shall be documented.

A statistically significant set of security audit data generated by the GPO-CA, since the last review, shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity. For the GPO-CA, at least 70% of security audit data generated by the GPO-CA since the last review shall be examined.

4.5.3 Retention Period for Security Audit Data

Audit logs shall be retained onsite for at least two months as well as being retained in the manner described below. The individual who removes audit logs from the GPO-CA system shall be an official different from the individuals who, in combination, command the GPO-CA signature key.

4.5.4 Protection of Security Audit Data

The audit process shall not be done by or under the control of the GPO-OA. GPO-CA system configuration and procedures must be implemented together to ensure that:

- only authorized people have read access to the logs
- only authorized people may archive audit logs
- audit logs are not modified

The entity performing audit log archive need not have modify access, but procedures must be implemented to protect archived data from destruction prior to the end of the audit log retention period (If a system over-writes audit logs after a given time, the audit log is not considered deleted or destroyed if the audit log has been backed up and archived). Audit logs shall be moved to a safe, secure storage location separate from the GPO-CA equipment.

4.5.5 Security Audit Data Backup Procedures

Audit logs and audit summaries shall be backed up at least weekly. A copy of the audit log shall be sent off-site in accordance with the GPO CPS on a weekly basis.

4.5.6 Security Audit Collection System (Internal vs. External)

The audit log collection system may or may not be external to the GPO-CA. Audit processes shall be invoked at system startup, and cease only at system shutdown. Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the GPO-OA shall determine whether to suspend GPO-CA operation until the problem is remedied.

4.5.7 Notification to Event-Causing Subject

This CP imposes no requirement to provide notice that an event was audited to the individual, organization, device, or application that caused the event.

4.5.8 Vulnerability Assessments

The Operational Authority will perform routine self assessments of security controls.

4.6 RECORDS ARCHIVAL

4.6.1 Types of Events Archived

GPO-CA archive records shall be sufficiently detailed to establish the proper operation of the GPO-CA, or the validity of any certificate (including those revoked or expired) issued by the GPO-CA.

At a minimum, the following data shall be recorded for archive in accordance with the GPO CP and CPS:

Data To Be Archived
GPO-CA accreditation (if applicable)
Certification Practices Statement
Contractual obligations
System and equipment configuration
Modifications and updates to system or configuration

Data To Be Archived
Certificate requests
Revocation requests
Subscriber identity Authentication data as per Section 3.1.9
Documentation of receipt and acceptance of certificates
Documentation of receipt of tokens
All certificates issued or published
Record of GPO-CA Re-key
All CARLs and CRLs issued and/or published
All Audit Logs
Other data or applications to verify archive contents
Certificate Policy
Other agreements concerning operation of the CA
Documentation required by compliance auditors

4.6.2 Retention Period for Archive

Archive data must be retained for a minimum of 10 years and 6 months. Executive branch agencies must follow either the General Records Schedule established by the National Archives and Records Administration or an agency-specific schedule as applicable. All other entities shall comply with their respective records retention policies in accordance with whatever laws apply to those entities.

This minimum retention period for these records is intended only to facilitate the operation of the GPO-CA.

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site. Alternatively, an Entity may retain data using whatever procedures have been approved by NARA for that category of documents. Applications that are required to process the archive data shall also be maintained for a period determined by the GPO-PA for the GPO-CA.

Prior to the end of the archive retention period, the GPO-CA shall provide archived data and the applications necessary to read the archives to a GPO-PA approved archival facility, which shall retain the applications necessary to read this archived data.

4.6.3 Protection of Archive

No unauthorized user shall be permitted to write to, modify, or delete the archive. For the GPO-CA, archived records may be moved to another medium when authorized by the GPO-OA. The contents of the archive shall not be released except as determined by the GPO-PA for the GPO-CA or as required by law. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. Archive media shall be stored in a safe, secure storage facility separate from the GPO-CA.

4.6.4 Archive Backup Procedures

No stipulation.

4.6.5 Requirements for Time-Stamping of Records

No stipulation.

4.6.6 Archive Collection System (Internal or External)

No stipulation.

4.6.7 Procedures to Obtain and Verify Archive Information

Procedures detailing how to create, verify, package, transmit, and store the GPO-CA archive information shall be published in the GPO CPS.

4.7 KEY CHANGEOVER

To minimize risk from compromise of a CA's private signing key, that key may be changed often; from that time on, only the new key will be used for certificate signing purposes. The older, but still valid, certificate will be available to verify old signatures until all of the certificates signed using the associated private key have also expired. If the old private key is used to sign CRLs that contain certificates signed with that key, then the old key must be retained and protected.

4.8 COMPROMISE AND DISASTER RECOVERY

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

If GPO-CA equipment is damaged or rendered inoperative, but the GPO-CA signature keys are not destroyed, GPO-CA operation shall be reestablished as quickly as possible, giving priority to the ability to generate certificate status information.

4.8.2 GPO-CA Signature Keys are Revoked

If the GPO-CA cannot issue a CARL/CRL prior to the time specified in the next update field of its currently valid CARL/CRL, then the GPO-PA and all of its members shall be securely notified as soon as practical. The GPO-CA shall reestablish revocation capabilities as quickly as possible in accordance with procedures set forth in the GPO CPS. The GPO-CA shall, as soon as practical, securely advise the GPO-PA and all of its member organizations in the event of a disaster where the GPO-CA installation is physically damaged and all copies of the GPO-CA signature keys are destroyed.

4.8.3 GPO-CA Signature Keys are Compromised

If the GPO-CA signature keys are compromised or lost (such that compromise is possible even though not certain):

- The GPO-PA and all of its member organizations shall be securely notified as soon as practical (so that Entities may issue CARLs revoking any cross-certificates issued to the GPO-CA)
- A new GPO-CA key pair shall be generated by the GPO-CA in accordance with procedures set forth in the GPO CPS
- New GPO-CA certificates shall be issued in accordance with the GPO CPS.

The GPO-CA governing body shall also investigate and report to the GPO-PA what caused the compromise or loss, and what measures have been taken to preclude recurrence.

4.8.4 Secure Facility Impaired After a Natural or Other Disaster

In the case of a disaster whereby the GPO-CA installation is physically damaged and all copies of the GPO-CA signature key are destroyed as a result, the GPO-PA and all of its member agencies shall be securely notified as soon as practical, and the GPO-PA shall take whatever action it deems appropriate. Relying Parties may decide of their own volition whether to continue to use certificates signed with the destroyed private key pending reestablishment of GPO-CA operation with new certificates.

4.9 CA TERMINATION

In the event of termination of the GPO-CA operation, certificates signed by the GPO-CA shall be revoked and the GPO-PA shall advise agencies that have entered into MOAs with the GPO-PA that GPO-CA operation has terminated so they may revoke certificates they have issued to the GPO-CA. Prior to GPO-CA termination, the GPO-CA shall provide archived data to a GPO-PA approved archival facility.

In the event that the GPO-CA terminates operation, the GPO-CA shall ensure that any certificates issued to the GPO-CA have been revoked.

5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS

5.1 PHYSICAL CONTROLS FOR THE GPO-CA

The GPO-CA shall impose physical security requirements that provide similar levels of protection as those specified below. All the physical control requirements apply equally to the GPO-CA.

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

5.1.1 Site Location and Construction

The location and construction of the facility housing the GPO-CA equipment shall be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, shall provide robust protection against unauthorized access to the GPO-CA equipment and records.

5.1.2 Physical Access

The GPO-CA equipment shall always be protected from unauthorized access, and especially while the cryptographic module is installed and activated. Physical access controls shall be implemented 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 equipment environment. Since the GPO-CA must plan to issue Medium Assurance certificates, it shall be operated and controlled at a minimum of a Medium Assurance Level.

Physical access controls and procedures shall be implemented to:

- Ensure no unauthorized access to the hardware is permitted
- Ensure 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 to both the cryptographic module and computer system

Removable cryptographic modules shall be inactivated prior to storage. When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules and GPO-CA equipment shall be placed in secure containers. Activation data shall either be memorized, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module.

A security check of the facility housing the GPO-CA equipment shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation
- 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

A person or group of persons shall be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance shall be maintained. If the facility is not continuously attended, both of the last two authorized personnel, to depart, will perform the check together, and both 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.

5.1.3 Electrical Power

The GPO-CA shall have backup capability sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. The directories (containing CA issued certificates and CARLs) shall be provided with uninterrupted power sufficient for a minimum of six (6) hours of operation in the absence of commercial power.

5.1.4 Water Exposures

Any stipulations will be specified in the GPO CPS.

5.1.5 Fire Prevention and Protection

Any stipulations will be specified in the GPO CPS.

5.1.6 Media Storage

GPO-CA media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic). Media that contains audit, archive, or backup information shall be duplicated and stored in a location separate from the GPO-CA.

5.1.7 Waste Disposal

Any stipulations will be specified in the GPO CPS.

5.1.8 Off-Site Backup

The GPO-CA requires, full system backups, sufficient to recover from system failure, shall be made on a periodic schedule, described in the GPO CPS. Backups are to be performed and stored off-site not less than once per week. At least one full backup copy shall be stored at an offsite location (separate from the GPO-CA equipment). Only the latest full backup need be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational GPO-CA.

5.2 PROCEDURAL CONTROLS FOR THE GPO-CA

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust for all uses of the GPO-CA. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

At a minimum the following roles will be used:

1. *GPO-OA System Administrator (GPO-OASA)* – authorized to install, configure, and maintain the CA; establish and maintain user accounts; and configure audit parameters
2. *GPO-OA Officer – Master Users* – authorized to configure certificate profiles; and generate component keys
3. *GPO-OA Officer – Security Officers* – authorized to manage (including issuance and revocation) Cross certificates, CA certificate and Trusted Role Subscriber certificates
4. *GPO-OA Officer– Administrators* – authorized to request or approve subscriber certificates or subscriber certificate revocations
5. *GPO-OA Officer – Directory Administrators* – maintaining the PKI entries in the certificate repository
6. *GPO Security Compliance Auditor* – authorized to view and maintain audit logs
7. *GPO-OA Backup Operator (GPO-OABUO)* – authorized to perform system backup and recovery

5.2.1.1 GPO-OA System Administrator

The administrator role is responsible for:

-
- installation, configuration, and maintenance of the CA
 - establishing and maintaining CA system accounts
 - configuring audit parameters

GPO-OASAs do not issue certificates to subscribers.

5.2.1.2 GPO OA Officer – Master Users

The OA Officer - Master Users are responsible for:

- configuring certificate profiles or templates
- generating and backing up CA keys

5.2.1.3 GPO OA Officer – Security Officers

The OA Officer - Security Officers are responsible for:

- registering new Trusted Role Subscribers and requesting the issuance of certificates
- verifying the identity of Trusted Role Subscribers and accuracy of information included in certificates
- approving and executing the issuance of Cross certificates, CA certificates and Trusted Role Subscriber certificates
- requesting, approving and executing the revocation of Cross certificates, CA certificates and Trusted Role Subscriber certificates

5.2.1.4 GPO OA Officer – Administrators

The OA Officer - Administrators are responsible for:

- registering new subscribers and requesting the issuance of certificates
- verifying the identity of subscribers and accuracy of information included in certificates
- approving and executing the issuance of subscriber certificates
- requesting, approving and executing the revocation of subscriber certificates

5.2.1.5 GPO OA Officer – Directory Administrators

The OA Officer - Directory Administrators are responsible for maintaining the PKI entries in the certificate repository. The Directory Administrator can be an OA Officer – Security Officer or OA Officer – Administrator, but may **not** be an OA Officer – Master User.

5.2.1.6 GPO Security Compliance Auditor

The auditor role is responsible for:

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

5.2.1.7 GPO Backup Operator

The operator role is responsible for the CA equipment system backups and recovery or changing recording media.

5.2.2 Separation of Roles

Role separation, when required as set forth below, may be enforced either by the CA equipment, or procedurally, or by both means. The separation provides a set of checks and balances over the GPO-CA operation.

CA personnel shall be specifically designated to the roles defined in Section 5.2.1 above. Individuals may assume more than one role, however, individuals who assume a Security Compliance Auditor role may not hold any other trusted role, individuals who assume an Officer role may not assume a System Administrator role (i.e. an Officer may also be a Backup Operator, a System Administrator may also be a Backup Operator). Individuals may not assume more than one of the following roles: OA Officer – Master User, OA Officer – Security Officer, or OA Officer – Administrator. The OA Officer – Directory Administrator may be an OA Officer – Security Officer or OA Officer – Administrator but may not be an OA Officer – Master User. The CA system shall identify and authenticate its users and shall ensure that no user identity can assume a Security Compliance Auditor role and any other role, or both a System Administrator and an Officer role. No individual shall be assigned more than one identity.

Under no circumstances shall the incumbent of a GPO-CA role perform its own auditor function.

5.2.3 Number of Persons Required Per Task

Multi person control is implemented to prevent accidental or malicious actions involving the GPO-CA. At a minimum the following actions require 2 or more individuals holding Trusted Roles:

- Generation of GPO-CA Signing Keys
- Activating GPO-CA Signing Keys
- Using GPO-CA Signing Keys
- Deactivating GPO-CA Signing Keys
- Backing up or Duplicating GPO-CA Private Signing Keys
- Physical Control of Backups of GPO-CA Signing Keys
- Physical Access or Control of the Cryptographic Module
- Physical Access or Control of the GPO-CA
- Physical Access or Control of the Safes and/or Secure Containers
- Physical Access to the GPO-CA
- Audit Log Review and Oversight
- Recovery of a subscribers encryption private key for a third party as directed by the GPO-CA Policy Authority or legal judgment

5.2.4 Identification and Authentication for Each Role

An individual shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity.

5.3 PERSONNEL CONTROLS

5.3.1 Background, Qualifications, Experience, and Security Clearance Requirements

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and must be U.S. citizens. The requirements governing the qualifications, selection and oversight of individuals who operate, manage, oversee, and audit the CA shall be set forth in the GPO CPS.

The GPO CPS will specify GPO-CA personnel security clearances stipulations.

5.3.2 Background Check Procedures

GPO background check procedures shall be described in the CPS and shall demonstrate that GPO requirements set forth in Section 5.3.1 are met.

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of the GPO-CA shall receive comprehensive training. Training shall be conducted in the following areas:

- CA/RA security principles and mechanisms
- All PKI software versions in use on the GPO-CA system
- All PKI duties they are expected to perform
- Disaster recovery and business continuity procedures
- Physical Security Procedures

5.3.4 Retraining Frequency and Requirements

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

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

The GPO-PA shall take appropriate administrative and disciplinary actions against personnel who have performed actions involving the GPO-CA or its repository not authorized in this CP, the GPO CPS, or other procedures published by the GPO-CA.

5.3.7 Contracting Personnel Requirements

Contractor personnel employed to perform functions pertaining to the GPO-CA shall meet applicable requirements set forth in section 5.3.1 above. Vendors who provide services to the GPO PKI shall establish procedures to ensure that any subcontractors who directly provide services to the GPO PKI perform in accordance with the requirements of section 5.3.1 above.

5.3.8 Documentation Supplied to Personnel

The GPO-CA shall make available to its CA and RA personnel the certificate policies it supports, relevant parts of the GPO CPS, and any relevant statutes, policies or contracts. Documentation shall be maintained identifying all personnel who received training and the level of training completed.

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 GPO-PKI and GPO-CA Key Pair Generation

Cryptographic keying material for certificates issued by the GPO-CA shall be generated in FIPS 140 validated cryptographic modules. For the GPO-CA, the modules shall meet or exceed Security Level 3.

The GPO-CA and Entity CAs must document their key generation procedure in their CPSs, and generate auditable evidence that the documented procedures were followed. The documentation of the procedure must be detailed enough to show that appropriate role separation was used. The process shall be validated by an independent third party.

6.1.2 Private Key Delivery to Subscriber

The GPO-CA generates its own key pair and therefore does not need private key delivery. GPO-CA Subscribers will usually generate their own signature keys and thus will not require delivery; where signature keys are generated by the GPO-CA, they will be delivered in accordance with this CP. For encryption keys, delivery of the private key to the Subscriber (or, if the Subscriber generates the encryption key pair, delivery by the Subscriber to the GPO-CA) shall be in accordance with the requirements of this CP.

6.1.3 Public Key Delivery to Certificate Issuer

Public keys shall be delivered to the certificate issuer in an authenticated manner set forth in the GPO CPS. This is usually via an electronic certificate request message from an RA, but it may also be done through other secure electronic mechanisms. Further, it may be accomplished via secure non-electronic means. These means may include, but are not limited to, floppy disk or other storage medium sent via registered mail or courier, or by delivery of a token to a certificate issuer for local key generation at the point of certificate issuance or request. If off-line means are used, they shall include identity checking as set forth in this CP and shall also ensure that proof of possession of the corresponding private key is accomplished.

6.1.4 GPO-CA Certificates and Public Key Availability and Delivery to Entity CAs

The GPO-CA shall post the certificates it issues in the GPO-CA repository. For Entity CAs to issue cross-certificates to the GPO-CA, the GPO-CA shall transport its public key to the Entity CA in a secure, out-of-band fashion to effect certificate issuance.

6.1.5 Key Sizes

All FIPS-approved signature algorithms shall be considered acceptable. If the GPO-PA determines that the security of a particular algorithm may be compromised, it may require the GPO-CA to revoke the affected certificates.

All certificates issued by the GPO-CA shall use at least 1024 bit RSA or Digital Signature Algorithm (DSA), with Secure Hash Algorithm version 1 (SHA-1) or better, in accordance with FIPS 186. GPO-CA use of Secure Socket Layer (SSL) or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum Triple-DES or equivalent for the symmetric key, and at least 1024 bit RSA or equivalent for the asymmetric keys.

6.1.6 Public Key Parameters Generation

Public key parameters prescribed in the Digital Signature Standard (DSS) shall be generated in accordance with FIPS 186.

6.1.7 Parameter Quality Checking

Parameter quality checking (including primarily testing for prime numbers) shall be performed in accordance with FIPS 186 or a more stringent test if specified by the GPO-PA.

6.1.8 Subscriber Key Generation

For subscribers, software or hardware shall be used to generate pseudo-random numbers, key pairs and symmetric keys. Any pseudo-random numbers used for key generation material shall be generated by a FIPS approved method.

6.1.9 Key Usage Purposes (as Per X.509 v3 Key Usage Field)

Public keys that are bound into certificates shall be certified for use in signing or encrypting, but not both, except as specified below. The use of a specific key is determined by the key usage extension in the X.509 certificate. In particular, certificates to be used for digital signatures (including authentication) shall set the *digitalsignature* and *nonrepudiation* bits. Certificates to be used for data encryption shall set the *dataencryption* bit. GPO-CA certificates shall set two key usage bits: *cRLSign* and *CertSign*. The GPO-CA certificates are only intended for signing of CRL's and signing of certificates. This restriction is not intended to prohibit use of protocols (like the Secure Sockets Layer) that provide authenticated connections using key management certificates.

Certificates may include a single key for use with encryption and signature in support of legacy Secure Multipurpose Internet Mail Extensions (S/MIME) applications. Such "dual-use" certificates shall not assert any of the Federal PKI Common Policy OIDs. Such "dual-use" certificates shall be generated and managed in accordance with their respective signature certificate requirements, except where otherwise noted in this CP. Such "dual-use" certificates

shall never assert the non-repudiation key usage bit, and shall not be used for authenticating data that will be verified on the basis of the dual-use certificate at a future time.

6.2 PRIVATE KEY PROTECTION

6.2.1 Standards for Cryptographic Module

The relevant standard for cryptographic modules is *Security Requirements for Cryptographic Modules* the latest version of FIPS 140 series. The GPO-PA may determine that other comparable validation, certification, or verification standards are sufficient. These standards will be published by the GPO-PA. Cryptographic modules shall be validated to the latest version of the FIPS 140 series level identified in this section or validated, certified or verified to requirements published by the GPO-PA. The minimum FIPS 140 requirements for cryptographic modules are as follows:

- Certification Authority (CA) - Level 3 Hardware
- Subscriber - Level 1 Hardware or Software
- Registration Authority (RA) - Level 2 Hardware

6.2.2 GPO-CA Private Key Multi-Person Control

Use of the GPO-CA private signing key shall require action by multiple persons as set forth in Section 5. of this CP.

6.2.3 Key Escrow of GPO-CA Private Signature Key

Under no circumstances shall the GPO-CA signature keys used to support non-repudiation services be escrowed by a third-party.

6.2.3.1 Escrow of CA Encryption Keys

The GPO-CA shall not perform any encryption key recovery functions involving encryption keys issued to Entity CAs.

6.2.4 Private Key Backup

6.2.4.1 Backup of GPO-CA Private Signature Key

The GPO-CA private signature keys shall be backed up under the same multi-person control as the creation of the original signature key. Such backup shall create only a single copy of the signature key at the GPO-CA location; a second copy may be kept at the GPO-CA backup location. Procedures for this shall be included in the GPO CPS.

6.2.4.2 Backup of Subscriber Private Signature Key

Subscriber private signature keys shall not be backed up, escrowed, or copied.

6.2.5 Private Key Archival

Private signature keys shall not be backed up, escrowed, or copied.

6.2.6 Private Key Entry Into Cryptographic Module

GPO-CA private keys shall be generated by and remain in a cryptographic module. The GPO-CA private keys may be backed up in accordance with Section 6.2.4.1.

6.2.7 Method of Activating Private Keys

The subscriber must be authenticated to the cryptographic module before the activation of any private key(s). Acceptable means of authentication include but are not limited to pass-phrases, PINs or biometrics. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

6.2.8 Private Key Deactivation Methods

If cryptographic modules are used to store private keys, then the cryptographic modules that have been activated shall not be left unattended or otherwise available to unauthorized access. After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure, or automatically after a period of inactivity as defined in the applicable GPO CPS. Hardware cryptographic modules shall be removed and stored in a secure container when not in use and not in the possession of the private key owner.

6.2.9 Private Signature Key Destruction Method

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

6.3 GOOD PRACTICES REGARDING KEY-PAIR MANAGEMENT

It is technically possible to use the same key-pair for both digital signature and confidentiality. However, this CP discourages that condition except to support legacy applications as defined in Section 6.1.9.

A subscriber’s key-pair that is used for digital signatures shall never be escrowed, archived or backed up, because a subscriber can repudiate a transaction if there is a copy of his or her digital signature private key in existence.

For information that is encrypted, the subscriber shall use his or her private encryption (confidentiality) key to decrypt the information. If that private key is lost or destroyed, or if the subscriber departs GPO without relinquishing the private key, or acts maliciously, there is no

way to decrypt the information. Thus, for business continuity reasons, GPO must be able to escrow, backup or archive private keys used for decrypting files and e-mails, while not escrowing, backing up or archiving key-pairs used for authentication. This means that two separate key pairs need to be employed.

6.3.1 Public Key Archival

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

6.3.2 Usage Periods for the Public and Private Keys

The GPO Subordinate CA (SCA) private signing key usage period will be 3 years (half of the 6 year certificate validity period). The GPO-SCA private signing keys will be used to sign certificates for 3 years. The certificates the GPO-SCA issues will be valid for at most 3 years.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

The activation data used to unlock GPO-CA or subscriber private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected. Activation data may be user selected. Activation data shall be generated in conformance with FIPS 112. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

6.4.2 Activation Data Protection

Data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data should either be biometric in nature or memorized, not written down. If written down, it shall be secured at the level of the data that the associated cryptographic module is used to protect, and shall not be stored with the cryptographic module. The protection mechanism shall include a facility to temporarily lock the account, or terminate the application after a predetermined number of login attempts as set forth in the GPO CP or CPS.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

The following computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The GPO-CA and its components shall include the following functionality:

- Require authenticated logins
- Provide Discretionary Access Control
- Provide a security audit capability
- Restrict access control to GPO-CA services and PKI roles
- Enforce separation of duties for PKI roles
- Require identification and authentication of PKI roles and associated identities
- Prohibit object re-use or require separation for GPO-CA random access memory
- Require use of cryptography for session communication and database security
- Archive GPO-CA history and audit data
- Require self-test security related GPO-CA services
- Require a trusted path for identification of PKI roles and associated identities
- Require a recovery mechanisms for keys and the GPO-CA system
- Enforce domain integrity boundaries for security critical processes

When GPO-CA equipment is hosted on evaluated platforms in support of computer security assurance requirements then the system (hardware, software, operating system) shall, when possible, operate in an evaluated configuration..

6.5.2 Computer Security Rating

No Stipulation.

6.6 LIFE-CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

The System Development Controls for the GPO-CA are as follows:

- The GPO-CA shall use software that has been designed and developed under a development methodology
- Hardware and software procured to operate the GPO-CA shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with

-
- Hardware and software developed specifically for the GPO-CA shall be developed in a controlled environment, and the development process shall be defined and documented (this requirement does not apply to commercial off-the-shelf hardware or software)
 - All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the GPO-CA physical location
 - The GPO-CA hardware and software shall be dedicated to performing one task: the GPO-CA. There shall be no other applications, hardware devices, network connections, or component software, which are not part of the GPO-CA operation
 - Proper care shall be taken to prevent malicious software from being loaded onto the GPO-CA equipment. Only applications required to perform the operation of the GPO-CA shall be obtained, from sources authorized by local policy. RA hardware and software shall be scanned for malicious code on first use and periodically afterward
 - 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.

6.6.2 Security Management Controls

The configuration of the GPO-CA system as well as any modifications and upgrades shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the GPO-CA software or configuration. A formal configuration management methodology shall be used for installation and ongoing maintenance of the GPO-CA system. The GPO-CA software, when first loaded, shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 NETWORK SECURITY CONTROLS

The Principal (root) GPO-CA shall not be connected to any network. The Subordinate GPO-CA shall be connected to at most one network. Use of appropriate boundary controls shall be employed, such as network guards, firewalls or filtering routers to guard against denial of service and intrusion attacks. Unused network ports and services shall be turned off. Any network software present shall be necessary to the functioning of the GPO-CA.

The GPO-CA CPS shall define the network protocols and mechanisms required for the operation of the GPO-CA Border Directory. Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

Requirements for cryptographic modules are as stated above in Section 6.2.1

7. CERTIFICATE AND CARL/CRL PROFILES

7.1 CERTIFICATE PROFILE

7.1.1 Version Numbers

The GPO-CA shall issue X.509 v3 certificates (populate version field with integer "2").

7.1.2 Certificate Extensions

Rules for the inclusion, assignment of value, and processing of extensions are defined in profiles. These profiles are written to prescribe an appropriate amount of control over an infrastructure, yet be flexible enough to meet the needs of the various CAs and communities. Certificates shall use *Federal PKI Version 1 Technical Specifications: Part E – X.509 Certificate and CRL Extensions Profile* [FPKI-Prof]. Whenever private extensions are used, they shall be identified in a CPS. Critical private extensions shall be interoperable in their intended community of use.

7.1.3 Algorithm Object Identifiers

Certificates issued under this CP shall use the following OIDs for signatures:

id-dsa-with-sha1	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3}
sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

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

id-dsa	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1}
RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
Dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}
id-keyExchangeAlgorithm	{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22}

7.1.4 Name Forms

Where required as set forth above, the subject and issuer fields of the base certificate shall be populated with an X.500 Distinguished Name, with the attribute type as further constrained by RFC2459.

7.1.5 Name Constraints

The GPO-CA shall assert name constraints in certificates it issues.

7.1.6 Certificate Policy Object Identifier

Certificates issued under this CP shall assert the OID appropriate to the level of assurance with which it was issued.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued under this CP shall not contain policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Processing semantics for the critical certificate policy extension used by the GPO-CA shall conform to the Federal Certificate Profile issued by NIST.

7.2 CARL/CRL PROFILE

7.2.1 Version Numbers

The GPO-CA shall issue X.509 version two (2) CARLs/CRLs.

7.2.2 CARL and CRL Entry Extensions

Detailed CARL/CRL profiles addressing the use of each extension shall conform to the Federal Certificate Profile issued by NIST.

8. SPECIFICATION ADMINISTRATION

8.1 SPECIFICATION CHANGE PROCEDURES

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

All policy changes under consideration by the GPO-PA shall be disseminated to interested parties. All interested parties shall provide their comments to the GPO-PA in a fashion to be prescribed by the GPO-PA.

8.2 PUBLICATION AND NOTIFICATION POLICIES

This CP and any subsequent changes shall be made publicly available within one week of approval.

8.3 CPS APPROVAL PROCEDURES

The term certification practices statement (CPS) is defined in the *Internet X.509 Public Key Infrastructure Certificate Policy and Certificate Practices Framework* as: "A statement of the practices, which a Certification Authority employs in issuing certificates." It is a comprehensive description of such details as the precise implementation of service offerings and detailed procedures of certificate life-cycle management. It shall be more detailed than the corresponding certificate policy described above. The GPO CPS, which is contained in a separate document published by the GPO-CA and approved by the GPO-PA, specifies how the GPO CP and any MOAs will be implemented to ensure compliance.

8.4 WAIVERS

The GPO-PA will develop and publish procedures pertaining to this area.

9. BIBLIOGRAPHY

The following documents were used in part to develop this CP:

- ABADSG Digital Signature Guidelines, 1996-08-01.
<http://www.abanet.org/scitech/ec/isc/dsgfree.html>
- FIPS 112 Password Usage, 1985-05-30
<http://csrs.nist.gov/>
- FIPS 140-1 Security Requirements for Cryptographic Modules, 1994-01
<http://csrs.nist.gov/fips/fips1401.htm>
- FIPS 140-2 Security Requirements for Cryptographic Modules, 2001-06
<http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>
- FIPS 180-1 Secure Hash Standard, 1995-04
<http://csrc.nist.gov/publications/fips/fips180-1/fip180-1.pdf>
- FIPS 180-2 Secure Hash Standard, 2002-08
<http://csrc.nist.gov/publications/fips/fips180-1/fip180-1.pdf>
- FIPS 186 Digital Signature Standard, 1994-05-19
<http://csrs.nist.gov/fips/fips186.pdf>
- FIPS 186-2 Digital Signature Standard, 2000-01
<http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf>
- FOIACT 5 U.S.C. 552, Freedom of Information Act.
<http://www4.law.cornell.edu/uscode/5/552.html>
- FPKI-Prof Federal PKI X.509 Certificate and CRL Extensions Profile
<http://csrc.nist.gov/pki/twg/y2000/papers/twg-00-18.xls>
- ISO9594-8 Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, 1997.
<ftp://ftp.bull.com/pub/OSIdirectory/ITU/97x509final.doc>
- ITMRA 40 U.S.C. 1452, Information Technology Management Reform Act of 1996.
<http://www4.law.cornell.edu/uscode/40/1452.html>
- NAG69C Information System Security Policy and Certification Practices Statement for Certification Authorities, rev C, November 1999.
- NSD42 National Policy for the Security of National Security Telecom and Information Systems, 5 Jul 1990.
http://snyside.sunnyside.com/cpsr/privacy/computer_security/nsd_42.txt
(redacted version)
- NS4005 NSTISSI 4005, Safeguarding COMSEC Facilities and Material, August 1997.
- NS4009 NSTISSI 4009, National Information Systems Security Glossary, January 1999.

- PKCS#12 Personal Information Exchange Syntax Standard, April 1997.
<http://www.rsa.com/rsalabs/pubs/PKCS/html/pkcs-12.html>
- RFC 2510 Certificate Management Protocol, Adams and Farrell, March 1999.
- RFC 2527 Certificate Policy and Certificate Practices Framework, Chokhani and Ford,
March 1999.
Security Requirements for Certificate Issuing and Management Components,
3 November 1999, Draft
Digital Signatures, W. Ford
- United States Department of Defense X.509 Certificate Policy, Version 5.0,
13 December 1999

10. ACRONYMS AND ABBREVIATIONS

CA	Certification Authority
CARL	Certificate Authority Revocation List
COMSEC	Communications Security
CP	Certificate Policy
CPS	Certification Practices Statement
CRL	Certificate Revocation List
CSOR	Computer Security Object Registry
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ERC	Enhanced Reliability Check
FAR	Federal Acquisition Regulations
FBCA	Federal Bridge Certification Authority
FBCA Operational Authority	Federal Bridge Certification Authority Operational Authority
FED-STD	Federal Standard
FIPS PUB	(US) Federal Information Processing Standard Publication
FPKI	Federal Public Key Infrastructure
FPKI-Prof	Federal PKI X.509 Certificate and CRL Extensions Profile
FPKISC	Federal PKI Steering Committee
FPKIPA	Federal PKI Policy Authority
GPEA	Government Paperwork Elimination Act of 1998

GPO-CA	Government Printing Office Certification Authority
GPO-CA Operational Authority	Government Printing Office Certification Authority Operational Authority
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ISSO	Information Systems Security Officer
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunications Sector
ITU-TSS	International Telecommunications Union – Telecommunications System Sector
MOA	Memorandum of Agreement (as used in the context of this CP, between an Entity and the GPO-PA allowing interoperation between the GPO-CA and Entity CA)
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OID	Object Identifier
PIN	Personal Identification Number
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SHA-1	Secure Hash Algorithm, Version 1

S/MIME	Secure Multipurpose Internet Mail Extension
SSL	Secure Sockets Layer
TSDM	Trusted Software Development Methodology
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
U.S.C.	United States Code
WWW	World Wide Web

11. GLOSSARY

Access	Ability to make use of any information system (IS) resource. [NS4009]
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009]
Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Agency	Any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Executive Branch of the Federal Government.
Agency CA	A CA that acts on behalf of an Agency, and is under the operational control of an Agency.
Applicant	The subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]
Archive	Long-term, physically separate storage.

Attribute Authority	An entity, recognized by the Federal PKI Policy Authority or comparable Agency body as having the authority to verify the association of attributes to an identity.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NS4009]
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009]
Backup	Copy of files and programs made to facilitate recovery if necessary. [NS4009]
Binding	Process of associating two related elements of information. [NS4009]
Biometric	A physical or behavioral characteristic of a human being.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]. As used in this CP, the term "Certificate" refers to certificates that expressly reference the OID of

this CP in the “Certificate Policies” field of an X.509 v.3 certificate.

Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CARLs or CRLs.
Certificate Authority Revocation List (CARL)	A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates, that have been revoked.
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies it’s Subscriber, (3) contains the Subscriber’s public key, (4) identifies it’s operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]
Certificate Management Authority (CMA)	A Certification Authority or a Registration Authority.
Certification Authority Software	Key Management and cryptographic software used to manage certificates issued to subscribers.
Certificate Policy (CP)	A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.

Certification Practices Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).
Certificate-Related Information	Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates.
Certificate Revocation List (CRL)	A list maintained by a Certification Authority of the certificates that it has issued and that are revoked prior to their stated expiration date.
Certificate Status Authority	A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.
Client (application)	A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.
Common Criteria	A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.
Component Private Key	Private key associated with a function of the certificate issuing equipment, as opposed to being associated as opposed to being associated with an operator or administrator.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]

Computer Security Objects Registry (CSOR)	Computer Security Objects Registry operated by the National Institute of Standards and Technology.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
Cross-Certificate	A certificate used to establish a trust relationship between two Certification Authorities.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS140]
Cryptoperiod	Time span during which each key setting remains in effect. [NS4009]
Data Integrity	Assurance that the data are unchanged from creation to reception.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made.
Dual Use Certificate	A certificate that is intended for use with both digital signature and data encryption services.
Duration	A field within a certificate that is composed of two subfields: "date of issue" and "date of next issue".

E-commerce	The use of network technology (especially the internet) to buy or sell goods and services.
Employee	Any person employed by an organization as defined above.
Encrypted Network	A network that is protected from outside access by NSA approved high-grade (Type I) cryptography. Examples are SIPRNET and TOP SECRET networks.
Encryption Certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.
End Entity	Relying Parties and Subscribers.
Entity	For purposes of this CP, Entity is any person, organization, corporation, or government (state, local, federal, or foreign) operating, or directing the operation of, one or more CAs.
Entity CA	A CA that acts on behalf of an Entity, and is under the operational control of an Entity.
Federal Bridge Certification Authority (FBCA)	The Federal Bridge Certification Authority consists of a collection of Public Key Infrastructure components (Certificate Authorities, Directories, Certificate Policies and Certification Practices Statements) that are used to provide peer-to-peer interoperability among Agency Principal Certification Authorities.

Federal Bridge Certification Authority Membrane	The Federal Bridge Certification Authority Membrane consists of a collection of Public Key Infrastructure components including a variety of Certification Authority PKI products, Databases, CA specific Directories, Border Directory, Firewalls, Routers, Randomizers, etc.
FBCA Operational Authority	The Federal Bridge Certification Authority Operational Authority is the organization selected by the Federal Public Key Infrastructure Policy Authority to be responsible for operating the Federal Bridge Certification Authority.
Federal Public Key Infrastructure Policy Authority (FPKI PA)	The Federal PKI Policy Authority is a federal government body responsible for setting, implementing, and administering policy decisions regarding interagency PKI interoperability that uses the FBCA.
Firewall	Gateway that limits access between networks in accordance with local security policy. [NS4009]
Government Printing Office Certification Authority (GPO-CA)	The Government Printing Office Certification Authority consists of a collection of Public Key Infrastructure components (Certificate Authorities, Directories, Certificate Policies and Certification Practices Statements) that are used to provide peer-to-peer interoperability among Other Certification Authorities.
GPO-CA Operational Authority	The Government Printing Office Certification Authority Operational Authority is the organization selected by the Government Printing Office Policy Authority to be responsible for operating the Government Printing Office Certification Authority.
High Assurance Guard (HAG)	An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.

Information System Security Officer (ISSO)	Person responsible to the designated approving authority for ensuring the security of an information system throughout its lifecycle, from design through disposal. [NS4009]
Inside threat	An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.
Integrity	Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.
Key Escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"]
Key Exchange	The process of exchanging public keys in order to establish secure communications.
Key Generation Material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.

Key Pair	Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.
Local Registration Authority (LRA)	A Registration Authority with responsibility for a local community.
Memorandum of Agreement (MOA)	Agreement between the GPO PKI Policy Authority and an Entity allowing interoperability between the Entity CA and the GPO-CA.
Mission Support Information	Information that is important to the support of deployed and contingency forces.
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see authentication).
Naming Authority	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
National Security System	Any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [ITMRA]

Non-Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009] Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal non-repudiation refers to how well possession or control of the private signature key can be established.
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI they are used to uniquely identify each of the four policies and cryptographic algorithms supported.
Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).
Outside Threat	An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.
Physically Isolated Network	A network that is not connected to entities or systems outside a physically controlled space.
PKI Sponsor	Fills the role of a Subscriber for non-human system components that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this CP.
Policy Management Authority (PMA)	Body established to oversee the creation and update of Certificate Policies, review Certification Practices 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. For the FBCA, the PMA is the Federal PKI Policy Authority.
Principal CA (PCA)	The Principal CA is a CA designated by an Agency to interoperate with the Entity CAs. An Agency may designate multiple Principal CAs to interoperate with the Entity CAs.
Privacy	Restricting access to subscriber or Relying Party information in accordance with Federal law and Organization policy.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).
Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.

Relying Party	A person or Agency who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.
Responsible Individual	A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.
Revoke a Certificate	To prematurely end the operational period of a certificate effective at a specific date and time.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Risk Tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Secret Key	A “shared secret” used in symmetric cryptography, wherein users are authenticated based on a password, Personal Identification Number

(PIN), or other information shared between the user and the remote host or server. A single key is shared between two parties: the sender, to encrypt a transmission, and the recipient, to decrypt the transmission, with the shared key being generated with an algorithm agreed to beforehand by the transacting parties.

Server

A system entity that provides a service in response to requests from clients.

Signature Certificate

A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.

Subordinate CA (SCA)

In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).

Additionally, this CP may refer to CAs that are “subordinate” to the PCA. The use of this term shall encompass any CA under the control of the PCA that has a certificate issued to it by the PCA or any CA subordinate to the PCA, whether or not a hierarchical or other PKI architecture is used.

Subscriber

A Subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual or network device

CAs are sometimes technically considered “subscribers” in a PKI. However, the term “Subscriber” as used in this document refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information.

Superior CA

In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (See subordinate CA).

System Equipment Configuration	A comprehensive accounting of all system hardware and software types and settings.
System High	The highest security level supported by an information system. [NS4009]
Technical non-repudiation	The contribution public key mechanisms to the provision of technical evidence supporting a non-repudiation security service.
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]
Token	Hardware or software that contains or can be used to generate cryptographic keys. Examples of hardware tokens include smart cards and memory cards. Software tokens include both software cryptographic modules that store or generate keys and storage devices or messages that contain keys (e.g., PKCS #12 messages).
Trust List	Collection of trusted certificates used by Relying Parties to authenticate other certificates.
Trusted Agent	Entity authorized to act as a representative of an organization in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.
Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".

Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
Trustworthy System	Computer hardware, software and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.
Two-Person Control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed, and each familiar with established security and safety requirements. [NS4009]
Update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
Zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS140]