U.S. GOVERNMENT PRINTING OFFICE
KEEPING AMERICA INFORMED

X.509 Certification Practices Statement for the U.S. Government Printing Office Principal Certification Authority (GPO-PCA)

September 17, 2014

FINAL

Version 1.7.4

FOR OFFICIAL USE ONLY

SIGNATURE PAGE

_____ _____

U.S. Government Printing Office DATE

Public Key Infrastructure Operating Authority

_____ _____

U.S. Government Printing Office DATE

Public Key Infrastructure Policy Authority Chair

TABLE OF CONTENTS

1. INTRODUCTION 1
1.1 OVERVIEW 2
1.1.1 Certificate Policy 2
1.1.2 Relationship Between the US Federal Common Policy and this CPS 2
1.1.3 Scope 2
1.1.4 Interoperation with CA's Issuing under Different Policies 3
1.2 DOCUMENT NAME AND IDENTIFICATION 3
1.3 PKI PARTICIPANTS 4
1.3.1 PKI Authorities 4
1.3.1.1 GPO PKI Policy Authority (PA) 4
1.3.1.2 GPO Operational Authority (OA) 4
1.3.1.3 GPO Operational Authority Oversight Administrator 5
1.3.1.4 GPO Operational Authority Officers 5
1.3.1.5 Entity Certification Authority 5
1.3.1.6 GPO Certification Authority 5
1.3.1.7 GPO Naming Authority 5
1.3.2 GPO Registration Authority (RA) 6
1.3.3 Trusted Agents 6
1.3.3.1 Related Authorities 6
1.3.3.1.1 Federal Bridge Certification Authority (FBCA) 6
1.3.3.1.2 Federal PKI Common Policy Root CA 6
1.3.4 Subscribers 6
1.3.5 Relying Parties 6
1.3.6 Other Participants 7
1.4 CERTIFICATE USAGE 7
1.4.1 Appropriate Certificate Uses 7
1.4.2 Prohibited Certificate Uses 7
1.5.3 Person Determining CPS Suitability for the Policy 8
1.5 POLICY ADMINISTRATION 8
1.5.1 Organization Administering the Document 8
1.5.2 Contact Person 8
The contact person for this CPS is the GPO Chief Information Security Officer, who can be reached by email at: pkisupport@gpo.gov. 8
1.5.3 Person Determining CPS Suitability for the Policy 8
1.6 DEFINITIONS AND ACRONYMS 9
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 9
2.1 REPOSITORIES 9
2.2 PUBLICATION OF CERTIFICATION INFORMATION 9
2.2.1 Publication of Certificates and Certificate Status 9
2.2.2 Publication of CA Information 9
2.2.3 Interoperability 10
2.3 TIME OR FREQUENCY OF PUBLICATION 10
2.4 ACCESS CONTROLS ON REPOSITORIES 10

3. IDENTIFICATION AND AUTHENTICATION 13
3.1 NAMING 13
3.1.1 Types of Names 13
3.1.2 Need for Names to be Meaningful 16
3.1.3 Anonymous or Psuedonymity of Subscribers 16
3.1.4 Rules for Interpreting Various Name Forms 16
3.1.5 Uniqueness of Names 16
3.1.5.1 Name Claim Dispute Resolution Procedure 16
3.1.6 Recognition, Authentication, and Role of Trademarks 16
3.2 INITIAL IDENTITY VALIDATION 16
3.2.1 Method to Prove Possession of Private Key 17
3.2.2 Authentication of Organization Identity 17
3.2.3 Authentication of Individual Identity 17
3.2.3.1 Authentication of Human Subscribers 18
3.2.3.1.1 Entrust Master Users 18
3.2.3.1.2 Entrust Officers 19
3.2.3.1.3 Entrust Administrators 19
3.2.3.1.4 GPO Registration Authorities 19
3.2.3.1.5 All Other Human Subscribers 19
3.2.3.2 Authentication of Devices 21
3.2.4 Non-Verified Subscriber Information 21
3.2.5 Validation of Authority 21
3.2.6 Criteria for Interoperation 21
3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS 22
3.3.1 Identification and Authentication for Routine Re-Key 22
3.3.2 Identification and Authentication for Re-Key After Revocation 22
3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST 22
3.4.1 Certificate Update 23
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 25
4.1 CERTIFICATE APPLICATION 25
4.1.1 Who Can Submit a Certificate Application 25
4.1.1.1 CA Certificates 25
4.1.1.2 User Certificates 25
4.1.1.3 Device Certificates 25
4.1.2 Enrollment Process and Responsibilities 25
4.2 CERTIFICATE APPLICATION PROCESSING 26
4.2.1 Performing Identification and Authentication Functions 26
4.2.2 Approval or Rejection of Certificate Applications 26
4.2.3 Time to Process Certificate Applications 26
4.2.4 Delivery of Public Key for Certificate Issuance 26
4.3 CERTIFICATE ISSUANCE 27
4.3.1 CA Actions During Certificate Issuance 28
4.3.2 Notification to Subscriber by the CA of Issuance of Certificate 28
4.3.3 GPO-PCA Subscribers Filling Trusted Roles 28
4.3.4 All Other Human Subscribers 28
4.3.5 Component and Server Subscribers 28

4.3.6 Delivery of Subscriber's Private Key to Subscriber 29
4.3.7 CA Public Key Delivery and Use 29
4.4 CERTIFICATE ACCEPTANCE 29
4.4.1 Conducting Constituting Certificate Acceptance 29
4.4.2 Publication of the Certificate by the CA 30
4.4.3 Notification of Certificate Issuance by the CA to Other Entities 30
4.5 KEY PAIR AND CERTIFICATE USAGE 30
4.5.1 Subscriber Private Key and Certificate Usage 30
4.5.2 Relying Party Public Key and Certificate Usage 30
4.6 CERTIFICATE RENEWAL 30
4.6.1 Circumstances for Certificate Renewal 31
4.6.2 Who May Request Renewal 31
4.6.3 Processing Certificate Renewal Requests 31
4.6.4 Notification of New Certificate Issuance to Subscriber 31
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 31
4.6.6 Publication of the Renewal Certificate by the CA 31
4.6.7 Notification of Certificate Issuance by the CA to Other Entities 31
4.7 CERTIFICATE RE-KEY 32
GPO-PCA Trusted Role Certificate Re-Key 32
CA Certificate Re-Key 32
4.7.1 Circumstance for Certificate Re-Key 33
4.7.2 Who May Request Certification of a New Public Key 33
4.7.3 Processing Certificate Re-keying Requests 33
4.7.3.1 Recovery of Security Officers 33
4.7.3.2 Recovery of Administrators 34
4.7.3.3 Recovery of Registration Authorities 34
4.7.3.4 Recovery of Subscribers 34
4.7.3.4.1 GPO-PCA Subscriber Certificate Re-Key 34
4.7.4 Notification of New Certificate Issuance to Subscriber 35
4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate 35
4.7.6 Publication of the Re-keyed Certificate by the CA 35
4.7.7 Notification of Certificate Issuance by the CA to Other Entities 36
4.8 CERTIFICATE MODIFICATION 36
4.8.1 Circumstances for Certificate Modification 36
4.8.2 Who May Request Certificate Modification 36
4.8.3 Processing Certificate Modification Requests 37
4.8.4 Notification of New Certificate Issuance to Subscriber 37
4.8.5 Conduct Constituting Acceptance of Modified Certificate 37
4.8.6 Publication of the Modified Certificate by the CA 37
4.8.7 Notification of Certificate Issuance by the CA to Other Entities 37
4.9 CERTIFICATE SUSPENSION AND REVOCATION 38
4.9.1 Circumstances for Revocation 38
4.9.2 Who Can Request Revocation 38
4.9.3 Procedure for Revocation Request 38
4.9.3.1 Revocation 39
4.9.4 Revocation Request Grace Period 39

4.9.5 Time within which CA must Process the Revocation Request ... 39
4.9.6 Revocation Checking Requirements for Relying Parties ... 39
4.9.7 Revocation List Issuance Frequency ... 39
4.9.7.1 CRL Checking Requirements ... 40
4.9.8 Maximum Latency for CRLs ... 40
4.9.9 On-line Revocation/Status Checking Availability ... 40
4.9.10 On-Line Revocation Checking Requirements ... 40
4.9.11 Other Forms of Revocation Checking ... 41
4.9.12 Special Requirements Related to Key Compromise ... 41
4.9.13 Circumstances for Suspension ... 41
4.9.14 Who Can Request Suspension ... 41
4.9.15 Procedure for Suspension Request ... 41
4.9.16 Limits on Suspension Period ... 41
4.10 CERTIFICATE STATUS SERVICES ... 41
4.10.1 Operational Characteristics ... 41
4.10.2 Service Availability ... 41
4.10.3 Optional Features ... 42
4.11 END OF SUBSCRIPTION ... 42
4.12 KEY ESCROW AND RECOVERY ... 42
4.12.1 Key Escrow and Recovery Policy and Practices ... 42
4.12.2 Session Key Encapsulation and Recovery Policy and Practices ... 42
5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS ... 43
5.1 PHYSICAL CONTROLS ... 43
5.1.1 Site Location and Construction ... 43
5.1.2 Physical Access ... 43
5.1.2.1 Physical Access for CA Equipment ... 45
5.1.2.2 Physical Access for Registration Authority Equipment ... 45
5.1.2.3 Physical Access for CSS Equipment ... 46
5.1.3 Power and Air Conditioning ... 46
5.1.4 Water Exposures ... 46
5.1.5 Fire Prevention and Protection ... 46
5.1.6 Media Storage ... 46
5.1.7 Waste Disposal ... 46
5.1.8 Off-Site Backup ... 47
5.2 PROCEDURAL CONTROLS ... 47
5.2.1 Trusted Roles ... 47
5.2.1.1 GPO OA System Administrator & Backup Operator (SABO) ... 48
5.2.1.2 GPO OA Officer – Master User ... 48
5.2.1.3 GPO OA Officer – Security Officer & Directory Administrator ... 49
5.2.1.4 GPO OA Officer – Registration Authority Administrator ... 49
5.2.1.5 GPO Security Compliance Auditor ... 49
5.2.1.6 Registration Authorities ... 50
5.2.2 Number of Persons Required Per Task ... 50
5.2.3 Identification and Authentication for Each Role ... 51
5.2.4 Roles Requiring Separation of Duties ... 56
5.3 PERSONNEL CONTROLS ... 56

5.3.1 Qualifications, Experience, and Clearance Requirements 56
5.3.2 Background Check Procedures 56
5.3.3 Training Requirements 57
5.3.4 Retraining Frequency and Requirements 57
5.3.5 Job Rotation Frequency and Sequence 58
5.3.6 Sanctions for Unauthorized Actions 58
5.3.7 Independent Contractor Requirements 58
5.3.8 Documentation Supplied to Personnel 58
5.4 AUDIT LOGGING PROCEDURES 59
5.4.1 Types of Events Recorded 59
5.4.2 Frequency of Processing Log 63
5.4.3 Retention Period for Audit Log 63
5.4.4 Protection of Audit Log 64
5.4.5 Audit Log Backup Procedures 65
5.4.6 Audit Log Collection System (Internal vs. External) 65
5.4.7 Notification to Event-Causing Subject 65
5.4.8 Vulnerability Assessments 65
5.5 RECORDS ARCHIVAL 66
5.5.1 Types of Events Archived 66
5.5.2 Retention Period for Archive 67
5.5.3 Protection of Archive 67
5.5.4 Archive Backup Procedures 68
5.5.5 Requirements for Time-Stamping of Records 68
5.5.6 Archive Collection System (Internal and External) 68
5.5.7 Procedures to Obtain and Verify Archive Information 68
5.6 KEY CHANGEOVER 68
5.7 COMPROMISE AND DISASTER RECOVERY 69
5.7.1 Incident and Compromise Handling Procedures 69
5.7.2 Computing Resources, Software, and /or Data are Corrupted 70
5.7.3 Entity (CA) Private Key Compromise Procedures 70
5.7.3.1 CA Signature Keys are Compromised 70
5.7.3.2 Secure Facility Impaired After a Natural or Other Type of Disaster 71
5.7.3.3 Notification Requirements for Disaster Recovery, Compromise and Incidents 71
5.7.4 Business Continuity Capabilities after a Disaster 71
5.8 CA OR RA TERMINATION 72
6. TECHNICAL SECURITY CONTROLS 73
6.1 KEY PAIR GENERATION AND INSTALLATION 73
6.1.1 Key Pair Generation 73
6.1.1.1 CA Key Pair Generation 73
6.1.1.2 Subscriber Key Pair Generation 73
6.1.1.3 Certificate Status Server (CSS) Key Pair Generation 73
6.1.2 Private Key Delivery to Subscriber 74
6.1.3 Public Key Delivery to Certificate Issuer 74
6.1.4 CA Public Key Delivery to Relying Parties 74
6.1.5 Key Sizes 74
6.1.6 Public Key Parameters Generation and Quality Checking 75

6.1.7 Key Usage Purposes (as per X.509 Key Usage Field) ... 75
6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS ... 75
6.2.1 Cryptographic Module Standards and Controls ... 75
6.2.2 Private Key Multi-Person Control (n out of m control) ... 77
6.2.3 Private Key Escrow ... 78
6.2.3.1 Escrow of CA Encryption Keys ... 78
6.2.4 Private Key Backup ... 78
6.2.4.1 Backup of GPO-PCA Private Signature Key ... 78
6.2.4.2 Backup of Subscriber Private Signature Key ... 78
6.2.4.3 Backup of Subscriber Private Key Management Key ... 79
6.2.4.4 Backup of Certificate Status Server (CSS) Private Key ... 79
6.2.5 Private Key Archival ... 79
6.2.6 Private Key Entry into or from a Cryptographic Module ... 79
6.2.7 Private Key Storage on a Cryptographic Module ... 79
6.2.8 Method of Activating Private Key ... 80
6.2.8.1 Access to Activated Cryptographic Modules and Private Key ... 80
6.2.8.2 Access to CA Cryptographic Modules When Not in Use ... 80
6.2.9 Method of Deactivating Private Key ... 81
6.2.10 Method of Private Key Destruction ... 81
6.2.11 Cryptographic Module Rating ... 81
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT ... 82
6.3.1 Public Key Archival ... 82
6.3.2 Certificate Operational Periods and Key Usage Periods ... 82
6.4 ACTIVATION DATA ... 83
6.4.1 Activation Data Generation and Installation ... 83
6.4.2 Activation Data Protection ... 84
6.4.3 Other Aspects of Activation Data ... 84
6.5 COMPUTER SECURITY CONTROLS ... 84
6.5.1 Specific Computer Security Technical Requirements ... 84
6.5.2 Computer Security Rating ... 85
6.6 LIFE CYCLE TECHNICAL CONTROLS ... 85
6.6.1 System Development Controls ... 85
6.6.2 Security Management Controls ... 85
6.6.3 Life Cycle Security Controls ... 86
6.7 NETWORK SECURITY CONTROLS ... 86
6.8 TIME-STAMPING ... 86
7. CERTIFICATE, CRL AND OCSP PROFILES ... 89
7.1 CERTIFICATE PROFILE ... 89
7.1.1 Version Numbers ... 89
7.1.2 Certificate Extensions ... 89
7.1.3 Algorithm Object Identifiers ... 89
7.1.4 Name Forms ... 90
7.1.5 Name Constraints ... 90
7.1.6 Certificate Policy Object Identifier ... 90
7.1.7 Usage of Policy Constraints Extension ... 90

7.1.8 Policy Qualifiers Syntax and Semantics 90
7.1.9 Processing Semantics for the Critical Certificate Policy Extension 90
7.2 CRL PROFILE 91
7.2.1 Version Numbers 91
7.2.2 CRL Entry Extensions 91
7.3 OCSP PROFILE 91
7.3.1 Version Numbers 91
7.3.2 OCSP Entry Extensions 91
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 92
8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT 92
8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR 92
8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY 92
8.4 TOPICS COVERED BY ASSESSMENT 92
8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY 93
8.6 COMMUNICATIONS OF RESULTS 94
9. OTHER BUSINESS AND LEGAL MATTERS 95
9.1 FEES 95
9.1.1 Certificate Issuance or Renewal Fees 95
9.1.2 Certificate Access Fees 95
9.1.3 Revocation or Status Information Access Fees 95
9.1.4 Fees for Other Services 95
9.1.5 Refund Policy 95
9.2 FINANCIAL RESPONSIBILITY 95
9.2.1 Insurance Coverage 95
9.2.2 Other Assets 95
9.2.3 Insurance or Warranty Coverage for End-Entities 96
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION 96
9.3.1 Scope of Confidential Information 96
9.3.2 Information Not Within Scope of Confidential Information 96
9.3.3 Responsibility to Protect Confidential Information 96
9.4 PRIVACY OF PERSONAL INFORMATION 96
9.4.1 Privacy Plan 96
9.4.2 Information Treated as Private 97
9.4.3 Information not Deemed Private 97
9.4.4 Responsibility to Protect Private Information 97
9.4.5 Notice and Consent to Use Private Information 97
9.4.6 Disclosure Pursuant to Judicial or Administrative Process 97
9.4.7 Other Information Disclosure Circumstances 98
9.5 INTELLECTUAL PROPERTY RIGHTS 98
9.6 REPRESENTATIONS AND WARRANTIES 98
9.6.1 CA Representations and Warranties 98
9.6.1.1 Certificate Issuance to Non-GPO Parties 99
9.6.1.2 Certificate Status Server Representations and Warranties 99
9.6.2 RA Representations and Warranties 100
9.6.3 Subscriber Representations and Warranties 100
9.6.4 Relying Party Representations and Warranties 100

9.6.5 Representations and Warranties of Other Participants 101
9.7 DISCLAIMERS OF WARRANTIES 101
9.8 LIMITATIONS OF LIABILITY 101
9.9 IDEMNITIES ..... ERROR! BOOKMARK NOT DEFINED.
9.10 TERM AND TERMINATION 102
9.10.1 Term 102
9.10.2 Termination 102
9.10.3 Effect of Termination and Survival 102
9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS 102
9.12 AMENDMENTS 102
9.12.1 Procedure for Amendment 102
9.12.2 Notification Mechanism and Period 103
9.12.3 Circumstances under which OID must be Changed 103
9.13 DISPUTE RESOLUTION PROVISIONS 103
9.14 GOVERNING LAW 103
9.15 COMPLIANCE WITH APPLICABLE LAW 103
9.16 MISCELLEANEOUS PROVISIONS 103
9.16.1 Entire Agreement 104
9.16.2 Assignment 104
9.16.3 Severability 104
9.16.4 Enforcement (Attorney's Fees and Waiver of Rights) 104
9.16.5 Force Majeure 104
9.17 OTHER PROVISIONS 104
10. BIBLIOGRAPHY 104
11. ACRONYMS AND ABBREVIATIONS 105
12. GLOSSARY 106
13. ACKNOWLEDGEMENTS 120
A.1 PCA (ROOT CA) SELF-SIGNED CERTIFICATE FORMAT 122
A.2 SUBORDINATE CA (SCA) CERTIFICATE FORMAT 123
A.3 EXTERNAL CA CERTIFICATE FORMAT 124
A.4 ROOT CA CRL PROFILE FORMAT 125
A.5 FEDERAL COMMON POLICY CERTIFICATE FORMAT 125
A.5.1 FEDERAL COMMON-HARDWARE CERTIFICATE FORMAT 126
A.5.2 COMMON POLICY SIGNATURE CERTIFICATE PROFILE 128
A.5.3 COMMON POLICY KEY MANAGEMENT CERTIFICATE PROFILE 129
A.5.4 COMMON POLICY DEVICE CERTIFICATE PROFILE 130
A.5.5 COMMON POLICY CARD AUTHENTICATION CERTIFICATE PROFILE 131
A.5.6 COMMON POLICY PIV AUTHENTICATION CERTIFICATE PROFILE 132
A.6.1 GPO MEDIUM ASSURANCE POLICY CERTIFICATE FORMAT 134
A.6.2 GPO MEDIUM-HARDWARE POLICY CERTIFICATE FORMAT 135
A.6.3 GPO POLICY END ENTITY SIGNATURE CERTIFICATE PROFILE 136
A.6.4 GPO POLICY KEY MANAGEMENT CERTIFICATE PROFILE 137
A.6.5 GPO POLICY MEDIUM DEVICE CERTIFICATE PROFILE 138
A.6.6 GPO POLICY CARD AUTHENTICATION CERTIFICATE PROFILE 139
A.6.7 GPO POLICY AUTHENTICATION CERTIFICATE PROFILE 140
A.7 GPO-PCA OCSP PROFILE FORMAT 142

A.8 GPO-PCA CERTIFICATE REGISTRATION DATA REQUIREMENTS 143

RECORD OF CHANGES

Version	Date	Author(s)	Reason	Description
1.0	December 9, 2003	CygnaCom Solutions	Initial Document	Initial Document
1.1	March 22, 2004	CygnaCom Solutions	Policy correction	Refine badge requirements for personnel filling GPO PKI Trusted Roles.
1.2	November 9, 2004	CygnaCom Solutions	Changes based on CP update	Address text modified in the CP
1.2.1	November 11, 2004	CygnaCom Solutions	Changes CP/CPS mapping	Align section numbering and address issues that may arise during an audit
1.2.2	November 11, 2004	CygnaCom Solutions	Correcting possible audit issues	
1.3	July 8, 2005	U.S. Government Printing Office	Responding to audit comments.	Minor changes. Removed Confidentiality Statement, added “For Official Use Only” classification to the document, and various other changes based on audit comments received from SeNet International Corporation.
1.4	February 27, 2006	U.S. Government Printing Office	Changes to comply with Federal PKI Common Policy and PKI Shared Service Provider (SSP) requirements	Changes to various sections required to comply with Common Policy requirements.
1.5	July 1, 2006	U.S. Government Printing Office	Changes to comply with AICPA WebTrust for CA auditor and GPO OIG audit recommendations.	Changes to various sections based on WebTrust for CA auditor and GPO OIG audit recommendations.
1.6	August 3, 2006	U.S. Government Printing Office	Minor changes to comply with GPO OIG and AICPA WebTrust for CA auditor recommendations.	Minor changes to a few sections based on GPO OIG and WebTrust auditor recommendations.
1.6.1	June 15, 2007	U.S. Government Printing Office	Minor changes to comply with GPO OIG and Compliance Auditor comments during annual compliance audit.	Minor changes to a few sections based on GPO OIG and Compliance Auditor comments during annual compliance audit.

Version	Date	Author(s)	Reason	Description
1.7	March 14, 2009	U.S. Government Printing Office	Updates to incorporate comments from SSPWG and NIST for Common Policy compliance during OCD, to incorporate additional GPO OID's, and to address comments from Compliance Auditor during CPS review against federal PKI Common Policy Compliance Matrix.	Changes to certain sections (Naming and Re-Key) to address comments submitted by SSPWG and NIST. Changes to various sections to incorporate issuance and management of Common-Common Policy OID's. Changes to various sections to incorporate additional GPO OID's (including GPO Medium-Hardware, GPO Authentication and GPO CardAuth) and compliance with GPO Certificate Policy, and to conform to RFC 3647 CPS format. Changes to address comments from Compliance Auditor.
1.7.1	June 3, 2011	U.S. Government Printing Office	Updates to incorporate FPKI approved changes to the Certificate Policy for the Federal PKI Common Policy Framework.	Update to certain sections for: aligning key length requirements with NIST SP 800-57; specifying controls for remote administration of the CA; inclusion of UUID's in Card Authentication certificates; clarifying archive definition and how its records are to be used; to clarify requirements for CA Key Rollover; and asserting policy OID's in OCSP Responder certificates for which the OCSP Responder is authoritative.
1.7.2	February 21, 2013	U.S. Government Printing Office	Updates to incorporate FPKI approved changes to the Federal PKI FBCA/Common Policy Framework.	Update to certain sections for: specification of allowed protocols for network security communications with the CA; activation data and installation; CA operating system (OS) software; personnel background check refresh; enrollment verification audit trail; and retaining FPKI cross-certification after CA key rollover.

Version	Date	Author(s)	Reason	Description
1.7.3	April 18, 2014	U.S. Government Printing Office	Updates to incorporate FPKI approved changes to the Federal PKI Common Policy Framework/FBCA CP.	Update to certain sections for: requiring PIV cards to be on the GSA APL; clarification of SHA-256 use; clarification of audit logging and log retention requirements; and clarification for the circumstances for CA and/or CSS certificate modification.
1.7.4	September 17, 2014	U.S. Government Printing Office	Updates to CRL issuing frequency.	Updates to section 4.9.7 for CRL issuing frequency.

1. INTRODUCTION

The Government Printing Office (GPO) has implemented a comprehensive Public Key Infrastructure (PKI) to provide the services necessary to enable the use of authentication, encryption, and digital signatures to secure GPO systems, communications, applications and data, and to enable the automation of inefficient and costly paper processes. In addition, the GPO intends for the GPO PKI to provide PKI Shared Services Provider (SSP) services, in compliance with all federal PKI requirements, to other agencies of the US federal government, as those agencies and the GPO PKI enter into the appropriate agreements to do so.

The PKI will provide certificates at any of the following levels of assurance as defined in the federal PKI Common Policy or the GPO Certificate Policy (GPO CP), as appropriate:

- Common (federal PKI Common Policy)
- Common Authentication (federal PKI Common Policy)
- Common Hardware (federal PKI Common Policy)
- Common Devices (federal PKI Common Policy)
- Common CardAuth (federal PKI Common Policy)
- GPO Medium Assurance (GPO Certificate Policy)
- GPO Medium-Hardware Assurance (GPO Certificate Policy)
- GPO Medium Assurance Devices (GPO Certificate Policy)
- GPO Authentication (GPO Certificate Policy)
- GPO CardAuth (GPO Certificate Policy)

The GPO PKI consists of products and services that provide and manage X.509 certificates for public key cryptography. Part of this PKI is a Certification Authority (CA) that generates and revokes X.509 public key certificates. The CA binds the Subscribers to their public/private key pairs, through the issuance of X.509 certificates.

The GPO PKI will consist of a Principle CA (GPO PCA), a Subordinate CA ((GPO SCA), and possibly further CA's. The federal PKI Common Policy and the GPO Certificate Policy (GPO CP) define the requirements for the creation and management of Version 3 X.509 public-key certificates for the GPO PKI. This Certification Practices Statement (CPS) defines the practices under which the GPO Principal CA (GPO-GPO-PCA) will operate. This CPS is applicable to all Subscribers, Relying Parties, and Registration Authorities of the GPO-PCA. This CPS provides these entities with a clear statement of the practices and responsibilities of the GPO-PCA, as well as the responsibilities of each entity in dealing with the GPO-PCA.

Security management services provided by the GPO-PCA include:

- Key Generation/Storage/Recovery
- Certificate and Certificate Revocation List (CRL) Generation and Distribution

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

The security and trustworthiness of the GPO-PCA depends on the security of the equipment, software, facilities, personnel, and procedures used in the operation of the GPO-PCA.

This CPS is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 3647, Certificate Policy and Certification Practice Statement Framework.

The practices specified in this CPS are described in more detail in the GPO PKI Operating Procedures document, which is incorporated by reference into this CPS.

1.1 OVERVIEW

Certificates from the GPO-PCA may be issued to GPO employees and contractors, and to GPO systems, devices and application processes, as required. The purpose of the GPO PCA is to provide an off-line Root CA for all GPO issued certificates and to principally issue certificates to subordinate CA's, in full compliance with all federal PKI Common Policy and PKI requirements and GPO CP requirements.. Encryption, authentication, and digital signature in support of non-repudiation key pairs will be supported. FIPS 140 certified software and hardware cryptographic modules will be used.

1.1.1 Certificate Policy

The practices described in this CPS are governed by and have been developed to support both the GPO Certificate Policy (GPO CP) and the federal PKI Common Policy. The requirements in this CPS are compliant with all aspects of both the federal PKI Common Policy and the GPO CP. In some cases, this CPS adds additional requirements to exceed to those in the federal PKI Common Policy and/or the GPO CP. . The federal PKI Common Policy and the GPO CP are incorporated into this document by reference.

1.1.2 Relationship Between the US Federal Common Policy and this CPS

This CPS is compliant with both the GPO Certificate Policy (GPO CP) and the federal PKI Common Policy in all respects.

1.1.3 Scope

This CPS applies to certificates issued by the GPO-PCA for subordinate CA's, and human subscribers and devices including any authorized affiliates (such as contracted personnel).

1.1.4 Interoperation with CA's Issuing under Different Policies

This CPS 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-PCA and the Entity CA In particular, this CPS facilitates interoperation of the GPO-PCA with the Federal Bridge CA and the Federal Common Policy Root CA. This CPS shall retain compliance with the federal PKI Common Policy and the GPO Certificate Policy (GPO CP) in all cases.

1.2 DOCUMENT NAME AND IDENTIFICATION

This document is known as the GPO Principal Certification Authority (GPO-PCA) Certification Practices Statement**.**

The practices stated herein conform to the specifications as defined both in the federal PKI Common Policy and the GPO Certificate Policy (GPO CP).

The GPO PCA will be responsible for issuing cross-certificates and subordinate CA certificates, when approved by the GPO Policy Authority (PA) and directed by the GPO Operational Authority (OA). There will also be a limited number of Subscriber certificates issued by the PCA. These Subscribers will consist of GPO and authorized GPO affiliate (contractor) individuals required to maintain and operate the PCA. Certificates that are created using these practices will assert the following policy Object Identifiers (OID):

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}
id-fpki-common-authentication	::= {2 16 840 1 101 3 2 1 3 13}
id-fpki-common-cardAuth	::= {2 16 840 1 101 3 2 1 3 17}
id-gpo-certpcy-mediumAssurance	::= {2 16 840 1 101 3 2 1 17 1}
id-gpo-certpcy-mediumHardware	::= {2 16 840 1 101 3 2 1 17 2}
id-gpo-certpcy-devices	::= {2 16 840 1 101 3 2 1 17 3}

id-gpo-certpcy-authentication	::= {2 16 840 1 101 3 2 1 17 4}
id-gpo-certpcy-cardAuth	::= {2 16 840 1 101 3 2 1 17 5}

The CA automatically populates the appropriate OID in certificate being issued in accordance with the practices of this CPS and the GPO PKI Operating Procedures.

This CPS complies with the requirements of the federal PKI Common Policy for the id-fpki-common-authentication and id-fpki-common-cardAuth (and therefore with the FIPS 201 requirements when those OID's are involved in certificates issued by the GPO-PCA). For certificates issued under the id-gpo-certpcy-authentication and id-gpo-certpcy-cardAuth OID's, the background check requirements of FIPS 201 do not apply, however, all other identity proofing requirements of the federal Common Policy are met.

1.3 PKI PARTICIPANTS

1.3.1 PKI Authorities

1.3.1.1 GPO PKI Policy Authority (PA)

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

- The GPO-PCA 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 federal PKI Common Policy (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-PCA, ensuring continued conformance of the Entity PKI Domain with applicable requirements is a condition for allowing continued interoperability with the GPO-PCA

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 CPS shall always refer to the Memorandum of Agreement cited in this paragraph.

1.3.1.2 GPO Operational Authority (OA)

The GPO Operational Authority (OA) is the organization that operates the GPO-PCA, including issuing GPO-PCA certificates when directed by the GPO-PA, posting those certificates and Certificate Revocation Lists (CRLs) into the GPO-PCA repository, and ensuring the continued availability of the repository to all users. The GPO-PCA Operational Authority includes the

following roles: Oversight Administrator, Officer, System Administrator, and Backup Operator, all described in later sections of this CPS.

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-PCA including the GPO-PCA repository, and who appoints individuals to the positions of GPO-PCA 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-PCA and its repository including executing GPO-PA direction to issue CA certificates to CAs or taking other action to effect interoperability between the GPO-PCA and Entity CAs.

1.3.1.5 Entity Certification Authority

An Entity wishing to interoperate with the GPO may apply for interoperation. Interoperation requires that a mapping between the Entity CP and the US federal PKI Common Policy and the GPO Certificate Policy must be completed, and that a Memorandum of Agreement (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-PCA and specify any additional requirements.

1.3.1.6 GPO Certification Authority

The GPO-PCA 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 and Subscribers. The GPO-PCA 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-PCA signing material
- Ensuring that all aspects of the GPO-PCA services, operations and infrastructure related to certificates issued under this CPS are performed in accordance with the requirements, representations, and warranties of this CPS

1.3.1.7 GPO Naming Authority

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

1.3.2 GPO Registration Authority (RA)

The GPO Registration Authority (RA) is the entity that collects and verifies each End Entity's identity and information to be entered into the subordinate CA certificate, or into the Subscriber's 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.

1.3.3 Trusted Agents

1.3.3.1 Related Authorities

1.3.3.1.1 Federal Bridge Certification Authority (FBCA)

This is a bridge CA for various legacy federal agency PKI systems under the Federal PKI framework.

1.3.3.1.2 Federal PKI Common Policy Root CA

This is the trust anchor (root CA certificate) for the federal PKI Shared Service Provider (SSP) program and federal PKI.

1.3.4 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.

1.3.5 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.

1.3.6 Other Participants

The GPO-PCA will require the participation of compliance auditors and assessors from time to time in accordance with this CPS and the applicable Certificate Policies, and may involve participation from personnel in the information security community in accordance with this CPS.

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Uses

Authorized applications are approved for the following security services provided by the GPO PKI:

- User Authentication
- Logical Access Control
- Secure Communication
- Digital Signature/Non-repudiation
- Card Authentication (card/token only; not presenter)

The GPO PA may identify additional authorized applications. This CPS will be updated as new authorized applications are identified.

1.4.2 Prohibited Certificate Uses

Applications that attempt to use these certificates for services other than those identified are prohibited. Certificates that assert the id-fpki-common-cardAuth OID shall only be used to authenticate the hardware token containing the associated private key, and shall not be interpreted as authenticating the presenter of the token, or the holder of the token.

1.5.3 Person Determining CPS Suitability for the Policy

The GPO-PA shall approve the GPO-PCA and its CPS. The GPO-PA is responsible for determining whether the GPO-PCA CPS conforms to the US federal PKI Common Policy and GPO CP, and in particular, properly adheres to any policy mappings approved by the GPO-PA.

1.5 POLICY ADMINISTRATION

Errors, updates, or suggested changes to this CPS document shall be communicated to the GPO OA. Such communication must include a description of the suggested change, contact information for the person requesting the change, and an impact assessment.

Notice of all changes to this CPS that may materially impact users of this CPS (other than editorial or typographical corrections) will be provided.

1.5.1 Organization Administering the Document

The GPO PKI Operational Authority (OA), which is performed and overseen by the GPO Information Technology and Systems (IT&S) organization, is the organization which administers this CPS document.

1.5.2 Contact Person

The contact person for this CPS is the GPO Chief Information Security Officer, who can be reached by email at: pkisupport@gpo.gov.

1.5.3 Person Determining CPS Suitability for the Policy

The Chair of the GPO Policy Authority (PA) and GPO Operational Authority Oversight Administrator are both responsible for determining the suitability of the CPS for the applicable Certificate Policy, which is the federal PKI Common Policy and GPO CP.

Changes to this document will be reviewed and approved by the PA.

The GPO PA will make the determination that this CPS complies with the US federal PKI Common Policy and the GPO Certificate Policy (GPO CP). The PA will also determine if a change to this CPS is acceptable and that the changed CPS continues to comply with the US federal PKI Common Policy.

The PA will provide written confirmation of CPS approval, which the PA will retain and make available for inspection during assessments and compliance audits.

1.5.4 CPS Approval Procedures

The GPO PA shall approve the CPS. The OA will deliver its CPS to the GPO PA for approval. Changes to this CPS shall also be coordinated with the federal Common Policy Framework approval authority, which is the Federal PKI Policy Authority.

1.6 Definitions and Acronyms

See sections 11 and 12 of this CPS.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 RESPOSITORIES

The repository for the GPO-PCA is an X.500 Directory and is accessed using the Lightweight Directory Access Protocol (LDAP) version 3, as specified in Internet RFC 1777, or via Hypertext Transport Protocol (HTTP). The GPO-PCA repository implements access controls and communication mechanisms (in the form of IP address controls) to prevent unauthorized modification or deletion of information.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

The GPO-PCA will publish the following information to the repository:

- All encryption and signature certificates issued by the GPO-PCA
- All CRLs issued by the GPO-PCA
- The GPO-PCA CA certificate

2.2.1 Publication of Certificates and Certificate Status

The GPO-PCA utilizes a set of redundant directory systems and Online Certificate Status Protocol (OCSP) servers to achieve high availability and meet the availability requirements of the federal PKI Common Policy and GPO CP. This is achieved both by on-site redundant directory systems at the primary GPO-PCA site, as well as backup directory systems, including an always online OCSP server, at the off-site backup location for the GPO-PCA.

2.2.2 Publication of CA Information

The GPO OA shall publish a copy of the GPO CP and the US Federal PKI Common Policy via the GPO PKI web site (http://www.gpo.gov/projects/pki.htm).

The GPO-PCA shall publish the CA certificate to the Repository. The Master Directory and the Shadow Directories reside on the GPO internal network behind one or more GPO controlled firewalls; all GPO or other authorized users shall have read-only access to the individual entries in the Shadow Directories.

The GPO-PCA application generates certificates and CRLs and has read, write and delete privileges to the master directory for PKI attributes. Directory Administrators and OA Officers have read, write and delete access for PKI-related attributes associated with individual entries in the master directory. The Master Directory information is automatically replicated to the shadow directories. Only the information which is designed to be publicly accessible is available from the Master Directory or the shadow directories, via use of Directory system access controls. Directory system access controls are used to protect all directory system information and ensure that publicly accessible and all other Directory system information is protected against unauthorized modification or dissemination.

2.2.3 Interoperability

Certificates, CRL's and Certificate Status Servers of the GPO-PCA shall use standards based protocols, data structure, and directory schemas, to ensure that interoperability with the federal PKI infrastructure (the federal Common Policy and Federal Bridge CA) and relying parties is achieved.

2.3 TIME OR FREQUENCY OF PUBLICATION

This CPS and any approved changes are published within 30 days of approval by the GPO PA.

Publication requirements for CRLs are described in sections 4.9.7 and 4.9.12 of this CPS.

Certificates are published in the directory as soon as they are issued. CRLs and ARLs are published in the directory as soon as they are issued.

The automated replication mechanism used internal to the Directory is configured to replicate any changes to the onsite redundant directory systems as soon the changes occur. Replication to the off-site backup Directory system shall occur at least once per day.

2.4 ACCESS CONTROLS ON REPOSITORIES

Direct and/or remote access to information in the Directory systems (Master Directory and shadow directories) other than the publicly accessible information shall be controlled via Directory system access controls to ensure that access is consistent with and compliant with the MOA that a customer agency has with the GPO-PCA. Only information specified in the agency MOA shall be automatically available via the GPO-PCA directory systems, and the MOA shall

define the user population that this applies to. Access to restricted information in the Directory systems (that information not designed to be automatically available via the agency MOA) is not generally available, and shall be discussed on a case by case basis with the Agency contact points in the MOA and any access that might be authorized must comply with the Federal PKI Common Policy requirements, the requirements of this CPS and the agency MOA, and shall be documented via hardcopy signed documents or digitally signed messages.

These access controls will be set with the native access control mechanisms of the Directory.

3. IDENTIFICATION AND AUTHENTICATION

This section contains the practices to be followed in identifying and authenticating the personnel who are responsible for the operation and maintenance of the GPO-PCA, and also defines the practices for identification and authentication of the subscribers and devices.

3.1 NAMING

3.1.1 Types of Names

The GPO-PCA uses the X.500 Distinguished Names (DN) for all Subscribers (which also complies with X.501 sub-standard of X.500). The DN may consist of naming elements C, O, OU and CN. The Naming Authority approved DN structures are as follows:

- For human Subscribers filling Trusted Roles for the GPO PKI:

  CN = [Subscriber first and last name, and *optionally*, a serial number] - The value of the serial number ***can*** be generated automatically to ensure uniqueness across all commonNames within a given directory path.
  OU = [Administrators]
  OU = [Government Printing Office]
  O = [U.S. Government]
  C = [US]
  Example: "**cn=John Smith + *serialNumber=A123456*, ou=Administrators, ou=Government Printing Office, o=U.S. Government, c=US**"

- For GPO human Subscribers:

  CN = [Subscriber first and last name, and *optionally*, a serial number] - The value of the serial number ***can*** be generated automatically to ensure uniqueness across all commonNames within a given directory path.
  OU = [Users]
  OU = [Government Printing Office]
  O = [U.S. Government]
  C = [US]
  Example: "**cn=John Smith + *serialNumber=A123456*, ou=Users, ou=Government Printing Office, o=U.S. Government, c=US**"
  NOTE: For federal contractors and other affiliated persons of GPO, the same structure as above shall be used except that the CN shall be constructed as follows:
  CN = [[Subscriber first and last name, and *optionally*, a serial number] (affiliate)] - The value of the serial number ***can*** be generated automatically to ensure uniqueness across all commonNames within a given directory path.

- For GPO Device Subscribers:

  CN = [device name and model number and the device serial number OR application name, and optionally, the application module number]
  OU = [Devices]
  OU = [Government Printing Office]
  O = [U.S. Government]
  C = [US]

  Example: "**cn=Cisco 12000 + *serialNumber=12XMZ4532*, ou=Devices, ou=Government Printing**

Office, o=U.S. Government, c=US"

- For GPO Application Subscribers:

  CN = [Application name, and optionally, the application module number]
  OU = [Applications]
  OU = [Government Printing Office]
  O = [U.S. Government]
  C = [US]

  Example: "**cn=Web Server Application + *serialNumber=Module 1*, ou=Applications, ou=Government Printing Office, o=U.S. Government, c=US**"

- For Other Agencies:

- For Other Agency human Subscribers:

  CN = [Subscriber first and last name, and *optionally*, a serial number] - The value of the serial number ***can*** be generated automatically to ensure uniqueness across all commonNames within a given directory path.
  OU = [Users]
  OU = [*OrgIdentifier*] – The value of the *OrgIdentifier* is going to be equal to the Other Agency name.
  O = [U.S. Government]
  C = [US]

  Example: "**cn=John Smith + *serialNumber=A123456*, ou=Users, ou=[Other *AgencyNam]e*, o=U.S. Government, c=US**"

  NOTE: For federal contractors and other affiliated persons of other Agencies, the same structure as above shall be used except that the CN shall be constructed as follows:
  CN = [[Subscriber first and last name, and *optionally*, a serial number] (affiliate)] - The value of the serial number ***can*** be generated automatically to ensure uniqueness across all commonNames within a given directory path.

- For Device Subscribers:

  CN = [device name and model number and the device serial number OR application name, and optionally, the application module number]
  OU = [Devices]
  OU = [*OrgIdentifier*] – The value of the *OrgIdentifier* is going to be equal to the Other Agency name
  O = [U.S. Government]
  C = [US]

  Example: "**cn=Cisco 12000 + *serialNumber=12XMZ4532*, ou=Devices, ou=[Other Agency Name], o=U.S. Government, c=US**"

- For Application Subscribers:

  CN = [Application name, and optionally, the application module number]
  OU = [Applications]
  OU = [*OrgIdentifier*] – The value of the *OrgIdentifier* is going to be equal to the Other Agency name

O = [U.S. Government]
C = [US]

Example: "**cn=Web Server Application + *serialNumber=Module 1*, ou=Applications, ou=[Other Agency Name], o=U.S. Government, c=US**"

Certificates for human subscribers may contain a subscriber alternate name form in the subjectAltName field. The subscriber alternate name will be the rfc822 e-mail address. For organization, device component and server Subscriber certificates, the subjectAltName field will be populated with the rfc822 e-mail address of the human sponsor.

CRL distribution points are named with the commonName attribute with a value generated by the CA application and are named subordinate to the GPO-PCA.

For certificates issued with the id-fpki-common-cardAuth OID, shall include a subject alternate name extension that includes the pivFASC-N type name type. The value for this extension shall be the FASC-N value of the subject's PIV card. In addition, the subject name for certificates issued with the id-fpki-common-cardAuth OID will be of the form:

Serial Number = [FASC-N]
OU = [Users]
OU = [*OrgIdentifier*] – The value of the *OrgIdentifier* is going to be equal to the Other Agency name.
O = [U.S. Government]
C = [US]

Example: "**S*erialNumber=FASC-N*, ou=Users, ou=[Other *AgencyNam]e*, o=U.S. Government, c=US**"

No certificate that contains the FASC-N in the subject alternative name extension or in the Serial Number shall be distributed via public directories.

PIV-I Card Authentication certificates shall indicate whether or not the Subscriber is associated with an Affiliated Organization by taking one of the following forms:

For certificates with an Affiliated Organization:

serialNumber=*UUID*, ou=Affiliated Organization Name, {Base DN}

For certificates with no Affiliated Organization:

SerialNumber=*UUID*, ou=Unaffiliated, ou=*Entity CA's Name*, {Base DN}

The UUID shall be encoded within the serialNumber attribute using the UUID string representation defined in section 3 of RFC 4122 (e.g., “f81d4fae-7dec-11d0-a765-00a0c91e6bf6”).

3.1.2 Need for Names to be Meaningful

The value of the commonName attribute used in naming a GPO-PCA Subscriber is the Subscriber’s first and last names.

The issuer name in CA certificates shall describe the GPO-PCA and shall be “cn=GPO-PCA”.

The subject name in CA certificates must match the issuer name in certificates issued by the subject, as required by RFC 3280, even if the subject’s name is not meaningful.

3.1.3 Anonymous or Psuedonymity of Subscribers

The GPO PCA shall not issue anonymous certificates. The GPO-PCA can issue pseudonymous certificates that identify subjects by their organizational role. The GPO-PCA shall not issue any CA certificate that is anonymous or pseudonymous.

3.1.4 Rules for Interpreting Various Name Forms

Distinguished names (DNs) and their component Relative Distinguished Names (RDNs) are to be interpreted in accordance with X.500 standards.

3.1.5 Uniqueness of Names

Names are unambiguously defined. The directory will be managed in such a way as to ensure that no two individuals are assigned the same DN, and therefore the same electronic identity. Name uniqueness is not violated when multiple certificates are issued to the same entity.

3.1.5.1 Name Claim Dispute Resolution Procedure

The PA is ultimately responsible for resolution of any name claim disputes within the GPO PKI. However, because the commonName attribute is considered unique within the GPO PKI repository, such naming conflicts are expected to be rare.

3.1.6 Recognition, Authentication, and Role of Trademarks

The RA will not knowingly assign names that contain trademarks. The RA need not seek evidence of trademark registrations nor in any other way enforce trademark rights.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

Public key certificates bind a public key to the identity of the individual to assure Relying Parties that signing performed by the private key was done by the individual whose public key appears on the certificate, and decryption using the private key can only be performed by the individual whose public key appears on the certificate. This requires that an individual safeguard their private key and any activation data used to access that key.

The CA requires proof of possession of the private key before creating and signing a certificate containing the associated public key. Proof of possession of a private key is handled automatically by CA to Subscriber messages protected by PKIX-Certificate Management Protocol (CMP).

For the Subscriber's signature private key, a PKIX-CMP operation initiated by the Subscriber is digitally signed using the signature private key itself.

For the Subscriber's decryption private key, the GPO-PCA generates both public and private keys so no proof of possession is required.

3.2.2 Authentication of Organization Identity

The certificates issued by the GPO-PCA to other CA's (subordinate CA certificates) will be issued according to the requirements defined in the US Federal PKI Common Policy, or the GPO CP, and this CPS. All certificate requests for subordinate CAs will include identity information of the requesting representative which will be forwarded to the GPO PA and federal PKI Policy Authority for approval. The federal PKI Policy Authority and GPO PA shall be notified whenever the GPO-PCA issues a CA certificate. All requests for CA certificates include identity information of the requesting representative which is forwarded to the GPO PA for approval. For a GPO subordinate CA, the request must come from the GPO OA and be approved in writing by the GPO PA. For an external agency subordinate CA, the request must come from an authorized representative as described in the agency MOA with the GPO-PCA, and the GPO OA or PA shall verify the request by contacting the authorized representatives of the requesting agency via telephone or in-person. A record of the authority verification including the method used (phone or in-person), the date, time, name of the person spoken with and signature of the GPO PA or OA, is kept by the PA and the OA.

A signed MOA with the agency provides the organization identity authentication information.

3.2.3 Authentication of Individual Identity

There are different classifications of Subscribers and the initial registration process differs accordingly as described in the sub-sections below; however, all Subscribers are responsible for providing identity-proofing credentials as part of the initial registration process. In general, the GPO PCA does not issue many certificates to individual end users, and when it does, in general this is only for the operation of the PCA and other GPO PKI operational requirements. A certificate shall be issued to a single entity. Certificates shall not be issued that contain a public key for which the associated private key is to be shared. The GPO-PCA issues certificates in accordance with the requirements of the US Federal PKI Common Policy for Common-Policy, Common-Hardware, Common-cardAuth, Common-Authentication, and Common-Devices

certificates and requires in-person proofing for all certificates issued under that policy. In addition, the GPO_PCA issues certificates in accordance with the GPO CP for Medium-Assurance, Medium-Hardware, GPO Authentication and GPO CardAuth, as appropriate based on the Subscriber request and procedures of this CPS.

3.2.3.1 Authentication of Human Subscribers

The acceptable identification documentation required by Subscribers is one Federal picture ID or two Non-Federal IDs, one of which must be a Government issued picture ID (i.e. State issued Drivers License or State issued Picture ID Card). A State issued Drivers License when presented by a Subscriber is checked against the U.S. Identification Manual (produced by Drivers License Guide Company) to ensure the ID has the proper format and appearance for the State involved. The RA compares the photograph on the Federal agency ID and the other form of government issued picture ID to the person standing in front of the RA and checks for a match. The photographs on the ID's are used to match to the person standing in front of the RA for in-person identity proofing. The RA also checks for any signs of tampering or fraud on all IDs presented by the Subscriber. If any signs of tampering or fraud are detected for any ID presented, the Subscriber is not registered for a certificate and the GPO PKI OA is contacted by the RA. In this event, the GPO PKI OA will send email to one of the contact points for the agency designated in that agency's MOA with the GPO PKI. The RA shall examine Federal agency IDs against the FIPS 201 standard, if the ID is recent enough (2006 on) to have been issued against that standard, to ensure that the photo and placement of text and graphics comply with the FIPS 201 requirements as way to detect fake IDs. The RA administrators shall check to ensure that the certificate registration information supplied by the subscriber matches the identification credentials supplied for in-person proofing, and that no errors are contained in the certificate registration information supplied by the subscriber. A biometric (either photograph or fingerprint) of the applicant (or human sponsor in the case of Common-Devices) shall be on file using official agency records and verified available to the CA and RA, or shall be captured at the time of enrollment by the OA or RA.

The following sections describe the initial registration processes for each of the classifications of Subscribers.

3.2.3.1.1 Entrust Master Users

All personnel holding Trusted Roles must complete and sign a Trusted Role Subscriber Agreement and a Registration Form and present, in person, two pieces of identification credentials, a GPO issued GPO Employee badge or GPO issued GPO Contractor badge and another government issued photo ID (such as a valid state issued Driver's license). The authentication is documented by a signed declaration from the PA or OAA that they personally verified the identity of the Subscriber in accordance with the requirements of this CPS, including the form of identification used, the identifying number of the ID and the date and time of the verification. A biometric of the applicant (either photograph or fingerprint) shall be captured by the OA at the time of enrollment.

3.2.3.1.2 Entrust Officers

All personnel holding Trusted Roles must complete and sign a Trusted Role Subscriber Agreement and a Registration Form and present, in person, two pieces of identification credentials, a GPO issued GPO Employee badge or GPO issued GPO Contractor badge and another government issued photo ID (e.g. a Driver's license). The authentication is documented by a signed declaration from two existing trusted users, a Master User and an existing Security Officer or two existing Security Officers that they personally verified the identity of the Subscriber in accordance with the requirements of this CPS, including the form of identification used, the identifying number of the ID and the date and time of the verification. A biometric of the applicant (either a photograph or fingerprint) shall be captured by the OA at the time of enrollment.

The initial Security Officer account, known as the First Officer, is created during the initial CA configuration. Two Master Users are responsible for authenticating the First Officer and verifying that the individual filling the role of First Officer properly completes the Trusted Role Subscriber Agreement and Registration Form. All subsequent Security Officers require authentication from at least two existing Security Officers, or one Security Officer and one Master User.

3.2.3.1.3 Entrust Administrators

To obtain their initial certificates, Administrators will enroll in person with two Security Officers. Administrators must complete and sign a Trusted Role Subscriber Agreement and a Registration Form and provide two pieces of identification credentials, a GPO issued GPO Employee badge or GPO issued GPO Contractor badge and another government issued photo ID (e.g. a Driver's license). A biometric of the applicant (either a photograph or a fingerprint) shall be captured by the OA at the time of enrollment. The authentication is documented by a signed declaration by the Security Officers that they personally verified the identity of the Subscriber in accordance with the requirements of this CPS, including the form of identification used, the identifying number of the ID and the date and time of the verification.

3.2.3.1.4 GPO Registration Authorities

GPO RAs can also be Entrust Administrators but are not necessarily Entrust Administrators. GPO RAs will enroll in person with an Entrust Administrator or GPO RA. RAs must complete and sign a Trusted Role Subscriber Agreement and a Registration Form and provide identification credentials, a GPO Employee picture ID. The GPO RA's employment by GPO shall be verified by the GPO Entrust Administrator or GPO RA, using official GPO records to accomplish this verification. The authentication is documented by a signed declaration by the Entrust Administrator or GPO RA that they personally verified the identity of the Subscriber in accordance with the requirements of this CPS, including the form of identification used, the identifying number of the ID and the date and time of the verification. A biometric of the GPO RA (either a photograph or a fingerprint) shall be on file using official GPO records and available at all times to the RA or CA, or be captured and maintained on file by the RA or the CA.

3.2.3.1.5 All Other Human Subscribers

To obtain their initial digital certificates, Subscribers will enroll in person with an RA. Subscribers must complete and sign a Subscriber Agreement and a Registration Form signed by the Subscriber's supervisor and provide identification credentials, one Federal picture ID, or two other forms of ID, at least one of which is a government issued photo ID (e.g. a State issued Driver's license). The validity of the supervisor's authority to sign the Registration Form shall be validated against official written communication (with paper signature) from an official agency Point of Contact (POC) as listed in the agency's MOA with the GPO PKI which lists authorized supervisors for that agency for this purpose. A digitally signed message from an official agency POC, using a certificate issued under this CPS, shall also be an acceptable method of written communication from the agency POC for the purpose of listing authorized supervisors for certificate registration. In addition, authentication of the sponsoring agency employee (POC) with a valid employee PIV-authentication certificate issued by the agency with valid cross-certification to the Federal PKI may be accepted as proof of both employment and identity. The MOA documents are digitally PCAnned by the GPO PKI OA into a fileshare that is available to the RA for the purpose of verifying the agency supervisor's validity. In addition, any digitally signed files received agency POC's are stored in this fileshare for RA use for this purpose. Also, the official paper copies of the MOA documents can also be reviewed by the RA as an acceptable method of verification. The Subscriber's employment by a federal agency shall be verified by the RA , using official agency records (the Subscriber's official agency employee ID badge) to accomplish this verification. The authentication is documented by a signed declaration by the RA that the RA personally verified the identity of the Subscriber in accordance with the requirements of this CPS, including the form of identification used, the identifying number of the ID, a declaration of identity signed by the certificate applicant using paper signature which is performed in the presence of the RA (in the format set forth at 28 U.S.C. 1746, which is the declaration under penalty of perjury), and the date and time of the verification. The GPO PKI Certificate Registration form (which is referenced and detailed in Appendix A3 of this CPS) is the form that must be used by the RA to record this information and the paper signature of the certificate applicant. A biometric of the Subscriber (either a photograph or a fingerprint) shall be captured and maintained on file by the RA or the CA (this shall be performed for agency contractors and other affiliated personnel). For agency contractors and other affiliated personnel, the authentication procedures shall require a digitally signed message from an agency employee using a GPO-PCA issued certificate, or shall require that authorized sponsoring agency employee also attends in-person for identity proofing and supplies the required identity documents. An authorized sponsoring agency employee for agency contractors or other affiliated personnel is defined to be personnel identified in the agency's MOA with GPO for this purpose, or by digitally signed message from those personnel in the MOA.

The GPO-PCA does not issue certificates that contain authorization or attribute information, therefore there is no verification process required or implemented associated with authorization or attribute information for a Subscriber.

Subscribers will use either hardware or software cryptographic module validated to at least FIPS 140 Level 1 for generating and storing their cryptographic credentials.

For certificates that assert organizational authority (such as the Chief Information Officer, or CIO, for example) the GPO-PCA shall validate the individual's authority to act in the name of the organization for this role. This shall be accomplished by examining the MOA for external

(non-GPO) entities and verifying that the MOA lists the subscriber as having the role an organizational authority to be asserted in the certificate, and for GPO, shall be accomplished by verification with the GPO Human Capital Office and documented via digitally signed message from the GPO Human Capital Office management personnel or via handwritten signature from GPO Human Capital Office management personnel.

3.2.3.2 Authentication of Devices

Applications for a device (component, device or server certificate) are made by an authorized human sponsor to whom the component or server's signature is attributable for the purposes of accountability and responsibility.

The human sponsor shall provide to the RA the following information about the component or device or server:

i) serial number (for devices)

ii) DNS and/or host name (for servers or components)

iii) Equipment public key

iv) Contact information for the human sponsor

Identification and authentication of the human sponsor follows Section 3.1.9 as if the sponsor were applying for a certificate on their own behalf. In addition, the RA will verify the authority of the sponsor to receive certificates for that component (device) or server. The authority of the sponsor to receive device or server certificates is defined to be those personnel identified for this purpose in the agency's MOA with GPO, or by digitally signed message from those personnel in the MOA.

3.2.4 Non-Verified Subscriber Information

Only verified information (verified by the RA or CA personnel) shall be included in certificates. The procedures specified in this CPS support this requirement.

3.2.5 Validation of Authority

Before issuing a certificate that asserts organizational identity, the GPO-PCA shall validate that the subscriber (applicant) has the authority to act in the requested capacity. This shall be validated by written statement of the authority from the organization involved. If this is a GPO organization, then a senior management official of the GPO Human Capital Office shall sign off on the authority authorization. If this is for a non-GPO organization, then an official specified in the MOA with the external agency shall sign off.

3.2.6 Criteria for Interoperation

The GPO-PCA shall follow the interoperability criteria set by the federal PKI Policy Authority (FPKIPA) for the federal Common Policy Root CA and Federal Bridge CA. For interoperability

with GPO customers not directly subject to the federal PKI infrastructure, the GPO-PCA shall follow the criteria set by the GPO PA and defined in the MOA with the external agency.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-Key

For CA re-key, the identification and authentication procedures shall be the same as for the initial process.

For all other certificates issued under this CPS, the Subscriber or device shall identify themselves for the purpose of routine re-key. The use of current, operational signature key may be used to establish identity and authentication for Subscribers and devices, except that in-person identity proofing must be accomplished after nine (9) years have elapsed since the last in-person proofing. The GPO-PCA shall have automated checks in the CA software (the Entrust Commerical Off the Shelf, COTS, CA software) to ensure that this nine (9) year requirement for in-person identity proofing is met.

The use of the current, operational signature key is used for identification and authentication via the use of the PKIX protocol, which provides for mutual authentication and data integrity, as implemented by the Entrust COTS software that is used by the GPO-PCA.

Should a Subscriber no longer be eligible for a GPO-PCA certificate, the Subscriber's account will be deactivated and the Subscriber's existing certificates will be revoked.

Once a routine re-key has been accomplished, the old certificate (which was replaced during the re-key shall not be further re-keyed or modified. The Enrust COTS CA software is used by the GPO-PCA to accomplish this control.

3.3.2 Identification and Authentication for Re-Key After Revocation

All GPO-PCA Subscribers or human sponsors (in the case of device certificates) must repeat the initial certificate registration and request process, and the initial identify proofing process, in order to obtain a new certificate after a revocation.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Revocation requests can be made by a Subscriber or another person authorized to act on behalf of the Subscriber (e.g., supervisor, HR department, etc.). All certificate revocation requests are communicated to an RA via secure means, either electronically or in person.

An RA may process a revocation request from a Subscriber, based on an email revocation request that has been digitally signed by the Subscriber.

An RA may process a revocation request based on a digitally signed email from an individual authorized to request revocation on behalf of the Subscriber (e.g. the Subscriber's supervisor, HR

representative, etc.). In this case, the RA will verify the authority of the requestor to submit the revocation request by validating the digital signature against an authoritative source.

An RA may process an in-person revocation request from a Subscriber, following authentication as outlined in Section 3.1.9.

3.4.1 Certificate Update

The GPO-PCA will support certificate update for name change. The applicant for certificate update must present himself or herself in person and provide proof of name change. After proof of name change a Distinguished Name (DN) change can be performed on the CA, this will issue a new certificate with the new name for the applicant.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 Who Can Submit a Certificate Application

4.1.1.1 CA Certificates

An applicant for a CA certificate must be an authorized representative of the organization requesting the CA certificate and shall be validated by the GPO OA. In the case of the GPO, this shall be a signed memorandum from the GPO PA. For non-GPO organizations, the validation shall consist of ensuring that a signed letter on organization letterhead, signed by an authorized representative as defined in the MOA between GPO and that agency, is on file and valid.

4.1.1.2 User Certificates

An application for a user certificate must be submitted by the user themselves or by an authorized trusted agent, in accordance with the procedures of this CPS.

Because all PCA Subscribers are individuals filling Trusted Roles, the GPO OA nominates the individuals to the GPO PA in a signed memorandum - electronic transmission with digital signature is permitted. The GPO PA authorizes (digital signature on the memorandum is permitted) the GPO OA to add the nominee to the appropriate Trusted Role in the directory and to approve a certificate for that nominee.

The signed certificate application is forwarded to the OA, who keeps a copy of all Subscriber certificate applications.

The OA forwards all completed requests for PCA certificates to the PA.

4.1.1.3 Device Certificates

The application for a device certificate must be submitted by the human sponsor for the device. In general, the GPO PCA does not issue device certificates since this is done by subordinate CA's.

4.1.2 Enrollment Process and Responsibilities

The enrollment process for the GPO-PCA uses out-of-band communication based upon the GPO PKI registration forms that are delivered and validated by the user or human sponsor during the

in-person identity proofing process. The form is presented and/or validated by the user or human sponsor in the presence of the Registration Authority.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 Performing Identification and Authentication Functions

The RA shall perform the identification and authentication function of certificate applicants using the practices of this CPS in section 3.

4.2.2 Approval or Rejection of Certificate Applications

Approval or rejection of certificate applications is performed by the RA, acting under the practices of this CPS.

4.2.3 Time to Process Certificate Applications

A certificate application shall be processed and if all criteria for issuance in accordance with this CPS are met, the certificate issued within 30 days of the certificate application being submitted and validated to the RA (during the in-person proofing process).

4.2.4 Delivery of Public Key for Certificate Issuance

Subscriber's encryption public keys are generated by the GPO-PCA, and are delivered to the Subscriber using the PKIX-CMP protocol to provide both integrity and privacy. The PKIX-CMP protocol between the CA and the software on the Subscriber's computer requires RSA 2048 bit public key encryption, AES-256 symmetric key encryption, and SHA-1 for hash algorithm. SHA-256 for hash algorithms will be required and used starting on or before January 1, 2008. The PKIX-CMP protocol prevents interception or substitution of data passed between the Subscriber's computer and the CA.

Subscriber signature verification public keys are generated on the Subscriber's token, and delivered to the GPO-PCA using the Entrust COTS PKI client software, which utilizes the PKIX-CMP protocol to provide both integrity and privacy of the communication.

4.3 CERTIFICATE ISSUANCE

The CA binds the identity information in the certificate application with the public keys during the certificate issuance process.

The Subscriber, using Entrust PKI COTS software provided by the RA at Subscriber in person registration and identity proofing (see section 3.1.9.6 above), initiates a PKIX-CMP protocol session with the CA to start the certificate issuance process. The Entrust PKI COTS software PKIX-CMP protocol cryptographic parameters are used. SHA-256 is to be used with the Entrust PKI COTS software PKIX-CMP protocol starting on January 1, 2008 and beyond. The PKIX-CMP protocol prevents interception of clear text data or substitution of data passed between the Subscriber's computer and the CA. The Reference Number and Authorization Code issued by the RA to the Subscriber during in-person identity proofing are entered by the Subscriber into the Entrust PKI COTS software at the Subscriber's PC, and this information uniquely identifies the Subscriber to the GPO-PCA. The Subscriber's Entrust PKI COTS software cryptographic module (which meets FIPS 140 Security Level 1 requirements) generates the Subscriber's public/private verification key pair, and submits the public key to the CA for certification using PKIX-CMP protocol. Upon receipt of a valid certificate request from the Subscriber over the PKIX-CMP session, the GPO-PCA automatically generates an encryption key pair and issues a signature verification public key certificate and an encryption public key certificate for that Subscriber, and this information is passed back to the Subscriber via the PKIX-CMP session.. The Subscriber certificates and the decryption private key, as well as the GPO-PCA's verification certificate , are provided to the Subscriber by the GPO-PCA using the PKIX-CMP protocol to provide both integrity and privacy, which also includes a specific message via the user interface to the Subscriber indicating success or failure of certificate issuance.

For certificates issued to subscribers on hardware tokens (smartcards, for example), an authorized PKI RA will issue the token to the subscriber. The token will be used along with the Entrust PKI COTS software, to interact with the CA using the PKIX-CMP protocol. The cryptographic parameters of the Entrust COTS software PKIX-CMP protocol are used. The token is created with the user present by the RA, then the user sets the password for the token, and the Subscriber then takes the token away at the successful conclusion of the certificate registration and issuance process. The Entrust PKI COTS software, which interfaces to the smartcard via standard PCKS #11 interface and to the CA via the standard Entrust COTS PKIX-CMP protocol, is used by the RA in order to accomplish the key generation and certificate issuance process. The Subscriber's verification public/private key pair is generated by the smartcard and the public key is submitted to the CA, via the PKIX-CMP session between the Entrust software on the RA workstation. Upon receipt of a valid certificate request over the PKIX-CMP session, the GPO-PCA automatically generates an encryption key pair and issues a signature verification public key certificate and an encryption public key certificate for that Subscriber, and this information is passed back to the token via the PKIX-CMP session. The 2 certificates are loaded into the token, using the Entrust PKI COTS software, and the token is ultimately handed to the Subscriber by the RA at the successful conclusion of the certificate issuance and registration process. The OA staff, in the form of the RA, shall securely maintain the stock of hardware tokens prior to issuance. The token serial number of any token issued to a subscriber shall be recorded on the certificate registration paperwork. Tokens may be re-used for other subscribers once the key destruction process, using the vendor supplied initialization and

key zeroization software, has been implemented by an authorized RA . Tokens associated with a key compromise event are not to be re-used. The Certificate Revocation Request Form has a check box to indicate to the RA that the reason for Revocation is Key Compromise and also has the Serial Number of the token involved, if a token applies. In the event of key compromise, the token (smartcard) is first zeriozed using the vendor zeroization software utility, and then the RA is to physically destroy the token by cutting it into at least 3 distinct pieces.

4.3.1 CA Actions During Certificate Issuance

The CA does not sign the certificate until all identify verification and authentication procedures described in this CPS are completed. This is ensured based on the procedure that is required by this CPS.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The CA notifies the Subscriber of the issuance of the certificate via the automated electronic communication that occurs between the CA and the Subscriber's client software (using PKIX-CMP protocol as implemented by the Entrust COTS software that the GPO-PCA uses). The Subscriber is notified explicitly by the messages displayed on the computer screen by the Subscriber PKI client software of the certificate issuance.

4.3.3 GPO-PCA Subscribers Filling Trusted Roles

The Trusted Role Subscriber uses the RA workstation to enter the reference number and authorization code provided during certificate application to complete the private key generation and certificate issuance process.

4.3.4 All Other Human Subscribers

The Subscriber uses the reference number and authorization code to complete the certificate issuance.

4.3.5 Component and Server Subscribers

Upon the completion of the certificate application, the human sponsor for the component or server Subscriber must generate the certificate request according to the component or server manufacturer's directions.

The human sponsor then submits the certificate request to the appropriate CA interface (i.e. Enrollment Server for VPN, Enrollment Server for Web, etc.) and authenticates the request with the reference number and authorization code provided during certificate application.

The CA interface then completes the certificate issuance process.

In some cases, PKIX-CMP may be supplemented by the use of other procedures such as Public Key Crypto Standard 10 (PKCS #10), or Cisco's Simple Certificate Enrollment Protocol (SCEP).

4.3.6 Delivery of Subscriber's Private Key to Subscriber

Subscribers generate their own private signature key, and as such, there is no need for delivery of the private signature key. The Entrust COTS PKI software, which meets FIPS 140 cryptographic module requirements, shall always be used by Subscribers that will have software certificates. Subscribers that will have hardware generated and stored private signature keys shall always use a FIPS 140 Security Level 2 (or greater) hardware token for this. RA Administrators are responsible for ensuing that the stock of hardware tokens for Subscribers are locked up and controlled from unauthorized access until the Subscriber is issued the token, during in-person identity proofing and certificate issuance.

Subscriber's private decryption keys shall always be delivered to the Subscriber from the GPO-PCA using the the Entrust COTS PKI CA and client PKI software, which always uses PKIX-CMP protocol to provide both integrity and privacy for the delivery process. The PKIX-CMP protocol as implemented by the Entrust COTS CA software provides for symmetric and asymmetric keys that are as strong or stonger than the Subscriber's private decryption key that is being communicated.

4.3.7 CA Public Key Delivery and Use

The GPO-PCA's verification certificate is provided to all Subscribers at the time of in-person identity proofing (per section 3.1.9 above) by the RA handing the Subscriber the certificate on a CD. The CA Public Key fingerprint value is also published on a web site controlled by the GPO PKI (http://www.gpo.gov/projects/pki.htm) as a method for relying parties to verify they have the proper GPO-PCA public key.

Relying Parties must also be granted access to the GPO-PCA's verification certificate, in order to establish and verify certification trust paths. In order to distribute the GPO-PCA verification certificate, the GPO-PCA publishes its verification certificate in the GPO PKI Repository.

4.4 CERTIFICATE ACCEPTANCE

All Subscribers submit a signed PKI Subscriber Agreement, which includes a Registration Form and the Subscriber Obligations. The Subscriber's signature on the PKI Subscriber Agreement will be deemed as the acceptance of the certificate and acceptance of the obligations and responsibilities as defined in the Subscriber Agreement.

The successful completion of the Certificate Issuance process constitutes the technical acceptance of the certificates.

4.4.1 Conducting Constituting Certificate Acceptance

The Subscriber accepts the certificate by continuing with the actions using the Subscriber client PKI software (Entrust COTS software) for certificate issuance. The Subscriber must notify the GPO-PCA in writing (email is acceptable) if the Subscriber does not accept for some reason the certificate, and must state the reason.

4.4.2 Publication of the Certificate by the CA

The GPO-PCA publishes the certificate into the GPO-PCA Directory system as soon as the certificate issuance is completed in concert with the Subscriber.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Publication of the certificate into the GPO-PCA directory and the availability of the certificate in that directory constitutes notification to other entities that the Subscriber's certificate exists and has been issued.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

The intended scope of usage for the private key and associated certificate for certificates issued by the GPO-PCA is specified through the use of certificate extension fields, including the key usage and extended key usage extension contained in issued certificates.

4.5.2 Relying Party Public Key and Certificate Usage

Certificates issued by the GPO-PCA make use of certain critical extensions, including key usage and basic constraints, in accordance with federal PKI Common Policy and GPO CP requirements, which relying parties are recommended to process and make use of in determining appropriate relying party use of GPO-PCA issued certificates. In addition, the GPO-PCA shall make available via the CRL and CSS service the status of certificates to relying parties (with the exception of OCSP Server certificates which are permitted to use the id-pkix-ocsp-nocheck extension), which relying parties are recommended to use in determining how to make use of any GPO-PCA issued certificate.

4.6 CERTIFICATE RENEWAL

The GPO-PCA does not support certificate renewal. If a Subscriber requires certificate renewal for any reason, the Subscriber will require a certificate re-key.

4.6.1 Circumstances for Certificate Renewal

No stipulation, since the GPO-PCA does not support certificate renewal.

4.6.2 Who May Request Renewal

No stipulation, since the GPO-PCA does not support certificate renewal.

4.6.3 Processing Certificate Renewal Requests

No stipulation, since the GPO-PCA does not support certificate renewal.

4.6.4 Notification of New Certificate Issuance to Subscriber

No stipulation, since the GPO-PCA does not support certificate renewal.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

No stipulation, since the GPO-PCA does not support certificate renewal.

4.6.6 Publication of the Renewal Certificate by the CA

No stipulation, since the GPO-PCA does not support certificate renewal.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation, since the GPO-PCA does not support certificate renewal.

4.7 CERTIFICATE RE-KEY

The GPO-PCA Subscriber keys are setup to be automatically re-keyed prior to expiration of the current key pair, based on possession of the non-expired private key. PKIX-CMP protected messages invoked by the GPO-PCA application update the Subscriber's keys transparently.

Re-authentication of the Subscriber's identity via in-person identify proofing, as defined in Section 3.2.3 of this CPS will be repeated within nine (9) years from the initial identity proofing, as required by the US Federal PKI Common Policy .

Re-key of a certificate does not require a change to the subjectName and does not violate the requirements for name uniqueness.

GPO-PCA Trusted Role Certificate Re-Key

The GPO-PCA Trusted Role keys are automatically updated prior to expiration of the current key pairs. If more than six (6) years have passed since the subscriber's identity was verified via in-person proofing (the procedures of section 3.2.3 above), then the certificate re-key shall require the same user identification proofing as certificate issuance.

The CA shall determine when certificate re-key operations will exceed the six (6) year limitation and therefore prevent the automatic re-key and require the subscriber to present themselves in person for identity proofing per section 3.2.3 above. The CA performs the following procedure to accomplish this:

a. Once per month, a listing is automatically created that lists all Subscribers who will pass the 6 year mark within the next 3 months.

b. All Subscribers on this list are sent an email informing them that they must present themselves for in-person identity proofing prior to the next 3 months.

c. The listing also shows any Subscribers that are active that have passed the 6 year mark, and thus in theory could have an automatic re-key performed. These Subscribers have their certificate revoked by the RA, and an email is sent to the user informing them that their certificate has been revoked and they must present themselves for in-person identity proofing (per section 3.1.9 above) to obtain another certificate or to have key recovery performed.

CA Certificate Re-Key

CA re-keys are manual processes and require a formal script that details the steps taken. The script must show that the required separation of roles was observed. The script will include a notification process for all CAs, RAs and subscribers that rely on the CA's certificate that it has been changed. The completed script is retained by the OA as an audit trail of the CA re-key operation. All individuals participating during a CA re-key are identified in the script and must present a valid government issued picture ID for verification of identity. All CA re-keys are authenticated during the re-key process, using the information in the certificate request and a thumbprint (MD5 Hash) received using a secure out-of-band method; these steps are part of the formal script.

For cross-certification relationships, no automatic key update process is applied. If the GPO PA determines that a cross-certification agreement is to extend beyond the original period, a new cross-certificate is issued, prior to expiration of the current one. Issuance of new certificate requires the same identification and authentication process used for the initial cross-certification.

4.7.1 Circumstance for Certificate Re-Key

Examples of situations that require a certificate re-key are hardware token failure, loss or compromise, or issuance of a new hardware token.

4.7.2 Who May Request Certification of a New Public Key

The RA may request certification of a new public key for subscribers. For device certificates, the human sponsor may request certification of a new public key.

4.7.3 Processing Certificate Re-keying Requests

When the existing, valid digital signature key cannot be used for accomplishing a certificate re-key via the PKIX CMP compliant process that the Entrust COTS software provides, then the following processing shall occur:

4.7.3.1 Recovery of Security Officers

When a Security Officer (applicant) needs certificate recovery, he/she must complete and sign a Certificate Recovery Request Form and present himself or herself in person to another Security Officer. The Security Officer performing the recovery will:

- Complete identification and authentication, as defined in Section 3.2.3
- Setup the applicant for certificate recovery
- Provide the shared secret data to the applicant
- Have the applicant create their profile
- Sign the Certificate Recovery Request Form indicating that they witnessed the applicant performing certificate recovery

The Certificate Recovery Request Form will be stored by the OA and will be made available during all compliance audits.

4.7.3.2 Recovery of Administrators

When an Entrust Administrator (applicant) needs certificate recovery, he/she must complete and sign a Certificate Recovery Request Form and present himself or herself in person to a Security Officer or another Administrator for recovery:

- Complete identification and authentication, as defined in Section 3.2.3
- Setup the applicant for certificate recovery
- Provide the shared secret data to the applicant
- Have the applicant create their profile
- Sign the Certificate Recovery Request Form indicating that they witnessed the applicant performing certificate recovery

The Certificate Recovery Request Form will be stored by the OA and will be made available during all compliance audits.

4.7.3.3 Recovery of Registration Authorities

An RA recovery is completed by:

- Complete a Recovery Request
- Identify and Authenticate RA to be recovered per requirements of section 3.2.3
- Setup RA for recovery
- Generate reference number and authorization code
- Have the RA recover their profile

Auditable information on all Certificate Recovery Requests will be stored by the OA and will be made available during all compliance audits.

4.7.3.4 Recovery of Subscribers

A Subscriber recovery is completed by:

- Complete a Recovery Request
- Identify and Authenticate Subscriber to be recovered per requirements of section 3.2.3
- Setup Subscriber for recovery
- Generate reference number and authorization code
- Have the Subscriber recover their profile

Auditable information on all Certificate Recovery Requests will be stored by the OA and will be made available during all compliance audits.

4.7.3.4.1 GPO-PCA Subscriber Certificate Re-Key

The GPO-PCA Subscriber keys, including Device certificates, are automatically updated prior to expiration of the current key pairs. If more than six (6) years have passed since the subscriber's

identity was verified via in-person proofing (the procedures of section 3.2.3 above), then the certificate re-key shall require the same user identification proofing as certificate issuance.

The CA shall determine when certificate re-key operations will exceed the six (6) year limitation and therefore prevent the automatic re-key and require the subscriber to present themselves in person for identity proofing per section 3.2.3 above. The CA performs the following procedure to accomplish this:

d. Once per month, a listing is automatically created that lists all Subscribers who will pass the 6 year mark within the next 3 months.

e. All Subscribers (Sponsors for Device certificates) on this list are sent an email informing them that they must present themselves for in-person identity proofing prior to the next 3 months.

The listing also shows any Subscribers that are active that have passed the 6 year mark, and thus in theory could have an automatic re-key performed. These Subscribers have their certificate revoked by the RA, and an email is sent to the user (the sponsor for a Device certificate0 informing them that their certificate has been revoked and they must present themselves for in-person identity proofing (per section 3.1.9 above) to obtain another certificate or to have key recovery performed.

4.7.4 Notification of New Certificate Issuance to Subscriber

The Subscriber is notified of the new certificate issuance by the messages displayed to the Subscriber while the Subscriber uses the client PKI software (Entrust COTS software) for certificate re-key. The Subscriber must notify the GPO-PCA in writing (email is acceptable) if the Subscriber does not accept for some reason the certificate, and must state the reason.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

The Subscriber accepts the certificate by continuing with the actions using the Subscriber client PKI software (Entrust COTS software) for certificate issuance. The Subscriber must notify the GPO-PCA in writing (email is acceptable) if the Subscriber does not accept for some reason the certificate, and must state the reason.

4.7.6 Publication of the Re-keyed Certificate by the CA

The GPO-PCA publishes the certificate into the GPO-PCA Directory system as soon as the certificate re-key is completed in concert with the Subscriber.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Publication of the certificate into the GPO-PCA directory and the availability of the certificate in that directory constitutes notification to other entities that the Subscriber's certificate has been re-keyed.

4.8 CERTIFICATE MODIFICATION

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-PCA may choose to update a certificate of a Subscriber whose characteristics have changed (e.g., name change due to marriage). The old certificate shall always be revoked, and therefore cannot 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. The new certificate shall have a new public key for cases in which an individual's name changes.

Finally, when the GPO-PCA updates its private signature key and thus generates a new public key, the GPO-PCA shall notify all the federal Common Policy CA, RAs, and subscribers that rely on the GPO-PCA's certificate that it has been changed. The GPO-PCA certificate is provided to subscribers during initial subscriber certificate issuance by having the RA distribute the GPO-PCA certificate on a CD.

4.8.1 Circumstances for Certificate Modification

The GPO-PCA may perform a certificate modification if the subscriber's characteristics change (for example, name change due to marriage).

The GPO-CA may modify a GPO CA or CSS (OCSP) certificate whose characteristics have changed, for instance, to assert a new policy OID. The new certificate may contain the same public key or a new public key.

4.8.2 Who May Request Certificate Modification

Subscribers with a currently valid certificate may request a certificate modification, by sending a digitally signed message. RA's may request a certificate modification on behalf of a subscriber, in the case in which an official agency record indicates that a name change or other modification event warrants this. For device certificates, the human sponsor of the device may request certificate modification.

4.8.3 Processing Certificate Modification Requests

If the subscriber's characteristics have changed (such as a name change), then official proof of the name change shall be verified by the RA. This can be accomplished via checking official agency records.

4.8.4 Notification of New Certificate Issuance to Subscriber

The Subscriber is notified of the new certificate issuance by the messages displayed to the Subscriber while the Subscriber uses the client PKI software (Entrust COTS software) for certificate modification. The Subscriber must notify the GPO-PCA in writing (email is acceptable) if the Subscriber does not accept for some reason the certificate, and must state the reason

4.8.5 Conduct Constituting Acceptance of Modified Certificate

The Subscriber accepts the modified certificate by continuing with the actions using the Subscriber client PKI software (Entrust COTS software) for certificate issuance. The Subscriber must notify the GPO-PCA in writing (email is acceptable) if the Subscriber does not accept for some reason the certificate, and must state the reason.

4.8.6 Publication of the Modified Certificate by the CA

The GPO-PCA shall publish all modified certificates into the GPO-PCA directory as specified above in section 2.2 of this CPS.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Publication of the modified certificate in the online, publicly accessible GPO-PCA directory shall constitute notification of certificate issuance to other entities, such as relying parties.

4.9 CERTIFICATE SUSPENSION AND REVOCATION

The GPO-PCA does not support suspension, and as such, the following sub-sections pertain strictly to certificate revocation.

4.9.1 Circumstances for Revocation

Certificates will be revoked when any of the following circumstances occur:

- Subscriber's private key is lost, stolen, suspected of compromise, or compromised
- Subscriber is suspected of fraud or other adverse behavior
- Subscriber leaves or is no longer affiliated with GPO or the sponsoring Agency
- Subscriber's identifying information contained in the certificate is no longer valid
- Subscriber violates the Subscriber Agreement
- Subscriber or other authorized party asks for Subscriber's certificate to be revoked

4.9.2 Who Can Request Revocation

The GPO PA or GPO-PCA OA can request revocation of any Subscriber certificate issued by the GPO-PCA. A written notice and brief explanation shall subsequently be provided to the affected Subscriber.

RAs can request revocation of a Subscriber's certificate. A Subscriber can always request revocation of a certificate in which they are listed as the certificate subject. A Subscriber's authorized Agency management official may request revocation.

4.9.3 Procedure for Revocation Request

When any of the circumstances for certificate revocation occur, the OA receives the revocation request and must process the request within the period specified in the US Federal PKI Common Policy.

The all revocation requests will review to ensure they are legitimate and will then revoke the certificate, as follows:

- Authenticate the person requesting revocation
- Verify the person requesting revocation is authorized to request revocation of the certificate in question
- Authenticate revocation request
- Revoke the certificate, specifying revocation reason
- Ensure the revocation request is kept by the OA

For GPO-PCA Subscribers using hardware tokens, the hardware token will be surrendered to the GPO-PCA OA and the GPO-PCA OA will zeroize the token using the token vendor provided utility.

4.9.3.1 Revocation

Revocation requests shall be processed and the CRL updated prior to the next CRL issuance, unless the revocation request is received within 2 hours of the next regularly scheduled CRL issuance. In that event (that the revocation request is received within 2 hours of the next regularly scheduled CRL issuance), the revocation shall be processed by the following CRL issuance. Certificate revocatioin takes effect upon the publication of the CRL (identifying the reason for the revocation, which may include loss, compromise, or termination of employment). Information about a revoked certificate shall remain on the CRL even after the certificate expires.

4.9.4 Revocation Request Grace Period

There is no grace period. The GPO-PCA shall revoke certificates upon request as quickly as is practical. Revocation requests shall be processed and the CRL updated prior to the next CRL issuance, unless the revocation request is received within 2 hours of the next regularly scheduled CRL issuance. In that event (that the revocation request is received within 2 hours of the next regularly scheduled CRL issuance), the revocation shall be processed by the following CRL issuance.

4.9.5 Time within which CA must Process the Revocation Request

Certificates that have been revoked shall **not** be removed from the CRL, they shall remain on the CRL even after the certificate expires. CRL's shall be issued by the GPO-PCA covering all certificates that have been revoked, with the only exception being for any OCSP Responder certificates issued that include the id-pkix-ocsp-nocheck extension.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying Parties determine what their revocation checking requirements are, using the application and business process risk as a factor in this determination.

4.9.7 Revocation List Issuance Frequency

The GPO-PCA server shall issue CRLs at least once every 20 days. CRL's are published to the repositories immediately upon generation. The nextUpdate time in the CRL shall be no longer than 10 days. The Entrust COTS CA software allows this 30 day maximum CRL lifetime to be enforced. Additional CRLs will be issued and published to the directory upon certificate revocation.

4.9.7.1 CRL Checking Requirements

Each certificate issued by the GPO-PCA includes the full DN of the CRL Distribution Point to be checked during the verification of the certificate. Relying parties, when working in an online mode, shall check the current CRL, identified by the DN in the certificate's cRLDistributionPoints extension field, along with any other CRLs required in certificate chain processing prior to trusting the certificate. Relying parties that use dated or out-of-date CRL's should not place as much trust in the certificates presented as when a current, valid CRL is checked. In order to have full trust in the certificates being checked, a current, valid CRL should be checked. If a dated (not current) or out-of-date CRL is the only CRL checked, then this additional risk is borne by the Relying Party.

When working in an offline mode, relying parties may not able to perform full CRL checking. When relying parties do not perform CRL checking, they accept the certificates at their own risk.

4.9.8 Maximum Latency for CRLs

CRL's are published as soon as they are generated. There is no latency intended between CRL generation and publication into the online GPO-PCA Directory system. Each CRL is published with the *nextUpdate* time specified in the previous CRL for the same scope. The Entrust COTS CA software allows this limit to be enforced.

4.9.9 On-line Revocation/Status Checking Availability

The GPO-PCA supports online status checking via OCSP in accordance with the IETF RFC 2560 standard. This is made available to support federal PKI Common Policy requirements for certificates issued with the id-fpki-common-authentication and id-fpki-common-cardAuth OID's. Status information is made available via this OCSP mechanism within 18 hours of certificate revocation.

4.9.10 On-Line Revocation Checking Requirements

The GPO-PCA does support on-line revocation/status checking using the OCSP protocol. Certificate status checking via the OCSP protocol can be performed for all OID types that are supported by the GPO-PCA..

OCSP data is updated every 30 minutes by the CA. The OCSP data available to relying parties is synchronized with the CA CRL every 30 minutes. Therefore, any certificate revocation is available to relying parties within 30 minutes of placement on the CRL.

A verification (signing) key issued by the GPO-PCA is used for the purpose of signing OCSP response messages.

Error messages in response to certificate status requests are not signed, as provided for in the IETF OCSP standard, RFC 2560.

4.9.11 Other Forms of Revocation Checking

No alternate methods of revocation advertisements are used.

4.9.12 Special Requirements Related to Key Compromise

CARLs are used to advertise CA private key compromise or loss.

4.9.13 Circumstances for Suspension

The GPO-PCA does not permit suspension for any type of certificate, including for CA certificates.

4.9.14 Who Can Request Suspension

The GPO-PCA does not permit suspension, therefore no one can request it..

4.9.15 Procedure for Suspension Request

The GPO-PCA does not permit suspension, therefore this is no procedure for this.

4.9.16 Limits on Suspension Period

No stipulation.

4.10 CERTIFICATE STATUS SERVICES

4.10.1 Operational Characteristics

The GPO-PCA provides CSS service via an online OCSP Responder in accordance with federal PKI Common Policy requirements and standard protocols.

4.10.2 Service Availability

The CSS for the GPO-PCA is available online and has an off-site backup system that is also online to provide operational resiliency and high availability to meet all federal PKI requirements.

4.10.3 Optional Features

No stipulation.

4.11 END OF SUBSCRIPTION

No stipulation.

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policy and Practices

CA keys are never escrowed.

Signature keys are never escrowed.

Subscriber key management keys are available for key recovery using the practices of this CPS.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

The GPO-PCA does not offer or perform this service/function.

5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

The GPO-PCA and Certificate Status Server (CSS) equipment is labeled as being for authorized use only. The GPO-PCA and CSS equipment are in a controlled facility that is monitored 24 hours per day, 7 days per week, 52 weeks per year. GPO-PCA and CSS cryptographic modules, both those active and operational, and those stored in security containers for on-site and off-site backup, are protected against theft, loss, and unauthorized use by the controls specified in section 5.1.2 below. All the physical control requirements specified below apply to the GPO-PCA and any remote workstations used to administer the CA's except where specifically noted (see section 5.1.2.1 below).

5.1.1 Site Location and Construction

GPO-PCA and Certificate Status Server (CSS) equipment, as well as remote workstations used to administer the CA's, are located in facilities approved by GPO as being appropriate for storing sensitive material. The GPO-PCA OA keeps a copy of documentation approving the GPO-PCA site including any remote workstations used to administer the CA's, and will provide the documentation for inspection during compliance audits.

5.1.2 Physical Access

Physical access controls and procedures are 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
- electronically monitor for unauthorized intrusion at all times
- Ensure an access log is maintained and inspected periodically
- Require via technical enforcement two-person physical access control to both the cryptographic module and computer systems

An integrated physical access control and intrusion detection system is operational to restrict access to authorized personnel, to detect unauthorized access, and to provide for the audit of all entries to and exits from the controlled areas. Sensors monitor exit and entrance doors.

The GPO Physical Access Controls system (Johnson Controls Incorporated, or JCI, Commercial Off-the-Shelf, COTS, software) controls all personnel access to the GPO PKI room, via use of door readers which requires a valid and authorized GPO Employee ID Badge to be presented. The door reader reads the magnetic stripe on the GPO Employee ID Badge and ensures that this badge is authorized to enter the PKI room. Authorized GPO PKI trusted role personnel must have their GPO Employee Badge entered into the GPO Physical Access Control System (Johnson Controls COTS software), as directed in writing via paper letter from the GPO Operational Authority to the Chief, GPO Security Service, by authorized GPO Physical Security Services staff.

Authorized GPO PKI trusted role personnel are required to badge into and out of the PKI Room and the PKI cage. Each door requires 2 valid and authorized parties for the door to open, both going into or out of the door.

The Security Zone is designated as a two-person zone. The GPO Physical Security Access Control System technically enforces the 2 person controls for physical access to the PKI room.

An access control policy is posted in the Operations zone and includes sign-in sheets for visitors. The policy requires all persons to wear an approved building pass and visitors to be escorted at all times within these high security zones.

Entrance to, and exit from, all controlled areas is monitored by closed circuit television (CCTV) and a system is used to record images or persons passing through the area. There is a CCTV camera outside the PKI Room door monitoring entry and exit from the PKI Room. There are two (2) CCTV cameras inside the PKI Room, monitoring the entry and exit into out of the PKI cage which further protects physical access to the PKI computer systems, including the CA system. In addition, an appropriate camera and time-lapse recorder will record activity in the security zone. The camera is placed such that persons in the room are recorded, but such that keystrokes typed on the system console may not be recovered by image enhancement. Images/recordings are maintained for a minimum of 90 days.

CA and CSS facilities are checked by the GPO Police at least once per business day to ensure that the physical protection mechanisms are still operating and ensure that there is no evidence of any breach of the physical security controls.. Records of these checks (including the names of the GPO Police Officer making the check, along with a date and time) are recorded by the GPO Physical Access Control System (Johnson Controls COTS software) and will be provided to the auditor during every compliance audit.

The door to the PKI Room and the door to the PKI cage are both instrumented to send an electronic alarm signal the GPO Police Command Center, which is manned 24 hours per day, 7 days per week, 52 weeks per year, in the event that the door is opened from either the outside or the inside without 2 valid Employee ID badges being presented for door opening. The GPO Police investigate all alarms that occur to ensure that no breach of physical securitiy to the PKI Room has occurred. The GPO Police have instructions to contact the GPO PKI Operational Authority (via cell phone) in the event that an alarm is generated to initiate and conduct investigation of the cause and response to the alarm.

Personnel are required to badge both going into, and coming out of the PKI Room and the PKI cage. 2 authorized badges must be presented at the reader for the door to open, going in either direction (into or out of the controlled space). The logs of the GPO Physical Access control system are reviewed on a monthly basis by the GPO Operational Authority and reconciled against the physical entry log (paper log) of the PKI Room. A GPO PKI Physical Access Review Form is filled out by the GPO Operational Authority on a monthly basis to document the results of the review and reconcilement process. If any inconsistencies are discovered in the reconcilement process, the GPO Operational Authority documents the results of the investigation in writing.

There are 2 security containers (safes which meet GSA security container requirements) stored inside the PKI Room, to implement split knowledge (2 party) controls in the secure storage of

PKI materials. The first safe can be accessed ONLY by those authorized personnel in the PKI Master User trusted role. The second safe can be accessed ONLY by those authorized personnel in the PKI Security Officer trusted role. Each safe has a hard copy log, which documents all entry into the safe, and records the reason the safe was opened, along with the date and time of opening and the time of closing and the person who opened the safe. The log is stored inside of the safe. Each safe also contains an inventory list of the materials that are contained in that safe. These 2 security containers protect media and sensitive paper documents from potential damage due to accident (for example, water damage, fire or electromagnetic damage), as well as providing physical access controls to prevent unauthorized access.

Secure container (safe) logs and inventory lists are reviewed and reconciled on a semi-annual basis (once every 6 months). The inventory reconciliation consists of verifying that each item on the inventory list is accounted for and stored in the safe.

Only trusted PKI personnel are given the keys, access cards, or the combination numbers required to access the CA equipment rooms/zones (as noted above visitors must sign in and will be escorted at all times).

The controls in this section of the CPS are operational and provide the controls for protecting the CA equipment from unauthorized access while the cryptographic module is installed and activated.

5.1.2.1 Physical Access for CA Equipment

The CA equipment is located in a secure PKI facility (at both the primary site and off-site backup location) which provides extensive controls over physical access as described in section 5.1.2. The remote workstations used to administer the GPO PCA are also protected via an extensive set of physical controls that include: a locked room under the control only of the authorized GPO PCA administrator personnel, security checks conducted every business day by the authorized GPO PCA administrator personnel and dual control enforcement for PCA access. Security checks are conducted and logged using GPO log books. There are no security containers located outside of the GPO PKI Room, and therefore there are no security containers in the room with remote workstations used to administer the PCA.

5.1.2.2 Physical Access for Registration Authority Equipment

Registration Authority equipment is protected from unauthorized access while the cryptographic module is installed via the password required for all RA tokens, which are required to be FIPS 140 Level 2 compliant hardware tokens. Only the authorized user can access the cryptographic module for RA operations, and the RA shall ensure that no other party uses the RA equipment while the RA is logged in. The RA user shall ensure that the Level 2 hardware token is controlled at all times, by having the token in the RA’s possession or in a locked cabinet/desk.

5.1.2.3 Physical Access for CSS Equipment

The CSS equipment is located in the secure PKI facility (at both the primary and off-site backup location) which provides extensive controls over physical access as described in section 5.1.2.

5.1.3 Power and Air Conditioning

All controlled access areas in the Security Zone shall be equipped with:

- An appropriately sized uninterruptible power supply (UPS) sufficient to allow for the systems to complete current actions and shutdown without data loss, and for six (6) hours of uninterruptible power for the directory servers
  - The UPS shall be sized to permit the CA to lock out input, finish any pending actions and record system state automatically
- Heating, ventilation, and air conditioning appropriate for a commercial data processing facilityEmergency lighting

These environmental controls shall conform to local standards and shall be appropriately secured to prevent unauthorized access and/or tampering with the equipment.

No liquid, gas, exhaust, etc. pipes shall traverse the controlled space other than those directly required for the area's HVAC system.

5.1.4 Water Exposures

The GPO-PCA and CSS equipment are installed such that it is not in danger of exposure to water. Sprinklers used for fire control have a contingency plan for recovery should the sprinklers malfunction, or cause water damage outside of the fire area.

5.1.5 Fire Prevention and Protection

The GPO-PCA and CSS secure facility is fully wired for fire detection, alarm and suppression. Routine, frequent inspections of all systems are made to assure adequate operation.

5.1.6 Media Storage

All media is stored away from sources of heat, and away from obvious sources of water (e.g., away from water pipes) or other obvious hazards. Electromagnetic media (tapes, diskettes, etc.) are stored away from obvious sources of strong magnetic fields (audio speakers, monitors). Archived material is stored in a room or building separate from the GPO-PCA and CSS equipment until it is transferred to the approved archive storage facility.

5.1.7 Waste Disposal

Sensitive media and documentation that are no longer needed and are to be destroyed shall be destroyed in a process that renders the material unrecoverable. Paper documents are shredded using a cross-cut shredder that complies with NSA/CSS 02-01. This shredder is located in the GPO Information Security office. Digital information on digital media that is to be disposed of is first sanitized using the Entrust TrueDelete COTS software, which complies with DoD and FIPS

standards for information cleaning/sanitization. Digital media that is to be destroyed shall be destroyed in accordance with DoD Standard 5220.22- M. Hard disks are to be mechanically destroyed after all information is sanitized. Magnetic tape is destroyed by first cutting the tape into at least 4 pieces and then running at least 2 of the pieces through a cross-cut shredder.

5.1.8 Off-Site Backup

Full system backups, sufficient to recover from system failure, are to be accomplished not less than once per week. A full system backup shall be stored at an off-site location (separate from the CA and CSS equipment), with physical controls commensurate with the operational CA.

The off-site backups are stored in locked containers, that have 2 separate padlocks. These locked containers are stored off-site using the Iron Mountain service. The off-site facility is located south of Springfield, VA in a facility that is monitored by Iron Mountain personnel on a 24 hour per day, 7 days per week, 52 weeks per year basis. The keys to the padlocks are controlled by 2 separate groups of authorized PKI trusted role personnel only, as follows; 1) The SABO has possession of 1 key to 1 of the padlocks; and 2) the Security Officer role has possession of the key to the other (second) padlock for the off-site backup media container. These containers also have tamper evident seals to indicate if the container has been opened.

The SABO and the Security Officer shall report any unauthorized break in the tamper evident seals to the GPO Operational Authority. In this event, the GPO Operational Authority shall conduct an investigation of the facts surrounding this and shall document the results in writing. There are two options for documenting the investigation and its results: 1) An official Problem Report logged in the GPO Help Desk Problem Tracking system; or 2) a written memorandum signed by the GPO Operational Authority.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

The GPO-PCA has the following Trusted Roles:

- OA System Administrator & Backup Operator
- OA Officer – Master User
- OA Officer – Security Officer & Directory Administrator
- OA Officer – Administrator
- Security Compliance Auditor

The following table identifies the way in which the required federal PKI Common Policy trusted roles map to the GPO-PCA Trusted Roles, and further to the Entrust product roles. As the table below shows, the GPO-PCA has further subdivided the federal PKI Officer trusted role into 3 distinct GPO Trusted Roles: 1) Master User; 2) Security Officer & Directory Administrator; and 3) Registration Authority Administrator.

Common Policy Role	GPO Role	Entrust Role
Administrator	OA System Administrator & Backup Operator	N/A

Common Policy Role	GPO Role	Entrust Role
	(SABO)	
Officer	OA Officer – Master User	Master User
	OA Officer – Security Officer & Directory Administrator	Security Officers (includes the First Officer) & Directory Administrator
	OA Officer – Registration Authority Administrator	Administrator
Auditor	Security Compliance Auditor	Auditor

Each GPO Trusted Role is explained in following sections.

5.2.1.1 GPO OA System Administrator & Backup Operator (SABO)

The OA System Administrator & Backup Operator (SABO) role is responsible for:

- installation, configuration, and maintenance of the CA and CSS
- establishing and maintaining CA and CSS system accounts
- configuring audit parameters for the CA and CSS
- configuring CSS response profiles
- supporting generation and backup of CA and CSS keys

The OA SABO is also responsible for performing backups, duplicating backups, secure storage of backups, and restoring from backups.

GPO-OA SABOs do not issue certificates to subscribers.

The OA SABO is responsible for initially installing and configuring the GPO-PCA operating system and for performing ongoing system administration duties such as account management, access control management, system configuration management, database maintenance, software upgrades, and compromise reporting.

5.2.1.2 GPO OA Officer – Master User

There are three Entrust Authority Master Users. Their Entrust Authority Master User passwords are documented and stored in a safe approved by the OA. The Master Users have authority to:

- Configuring certificate profiles or templates
- Generating and backing up CA keys
- Maintain Entrust Authority services (consisting of Administration Service and Key Management Service) plus the Entrust Authority database
- Recover the Entrust Administration service, in the event its profile becomes damaged
- Backup, re-encrypt and restore from backup as necessary, the Entrust Manager database

5.2.1.3 GPO OA Officer – Security Officer & Directory Administrator

The Entrust Security Officer created during the installation of the Entrust Authority is the *First Officer*. The First Officer, drawing from selected GPO personnel, creates additional Entrust Security Officers. The main role of an Entrust Security Officer is to set and administer the GPO-PCA's security policy as it applies to all Subscribers. Entrust Security Officers have the following privileges:

- Verifying the identity of Trusted Role Subscribers and accuracy of information included in certificates
- Set the security policy for the GPO-PCA, and alter it
- Add, delete and revoke other Entrust Security Officers, Entrust Administrators, and Directory Administrators
- Authorize sensitive operations, such as adding and deleting Security Officers and Administrators

The names of the Security Officers will be made available to the Compliance Auditor during each compliance audit.

The Security Officer & Directory Administrator is also responsible for maintaining the certificate repository.

5.2.1.4 GPO OA Officer – Registration Authority Administrator

For the GPO-PCA, the Registration Authority Administrators are responsible for:

- Verifying the identity of GPO-PCA Subscribers
- Securely communicating requests to and responses from the CA
- Executing revocation requests received from authorized sources

The names of the Registration Authorities will be made available to the Compliance Auditor during each compliance audit.

5.2.1.5 GPO Security Compliance Auditor

The Security Compliance Auditor role is responsible for:

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

The Security Compliance Auditor also known as the Security Compliance Officer (SCO) is responsible for reviewing, but not modifying audit logs, various reports, Security Policy and user properties. The Security Compliance Auditor is responsible for performing or overseeing internal compliance audits to ensure that CA is operating in accordance with its CPS

The names of the Security Compliance Auditor(s) will be made available to the Compliance Auditor during each compliance audit.

5.2.1.6 Registration Authorities

For the GPO-PCA, the Registration Authorities are responsible for:

- Verifying the identity of GPO-PCA Subscribers
- Registering new subscribers and requesting the issuance of certificates
- Securely communicating requests to and responses from the CA and approving the issuance of certificates
- Approving, requesting when appropriate and executing revocation requests received from authorized sources

The names of the Registration Authorities will be made available to the Compliance Auditor during each compliance audit.

A Local Registration Authority (LRA) may verify the identity of Subscribers during the registration process. LRAs are individuals appointed and/or recognized by the OA.

5.2.2 Number of Persons Required Per Task

All Entrust Security Officer operations need at least one Security Officer authorization. Certain functions, such as activation of the CA Private Key, will be protected by multi-person controls. The following operations need two authorizations:

- Generation of GPO-PCA Signing Keys
- Activation of GPO-PCA Signing Keys
- Using GPO-PCA Signing Keys
- Deactivation of GPO-PCA Signing Keys
- Backing up or Duplicating of GPO-PCA Private Signing Key
- Physical Control of Backups of GPO-PCA Signing Keys
- Physical Access or Control of the Cryptographic Module
- Physical Access or Control of the GPO-PCA
- Physical Access or Control of the GPO-PCA Safes and/or Secure Containers
- Physical Access to the GPO-PCA Signing Keys
- Adding and deleting Security Officers
- Setting default certificate lifetimes
- CA master key updates
- Recovery of Administrator and Officer accounts
- CA hardware, OS, and application software maintenance

5.2.3 Identification and Authentication for Each Role

Systems Administrators do not have access to the Security Manager Administration application.

Since GPO intends to have the GPO-PCA issue certificates as a service to other Entities, and allow them to have RAs, and LRAs that administer the certificates issued to Entity Subscribers, the RA and LRA privileges will be determined based on the requirements of this CPS and the agreement with the Entity.

The following table identifies the GPO Trusted Roles and the privileges assigned to each role within the Entrust CA:

Privilege	**Trusted Roles**			
	OA Officer Master Users	**OA Officer Security Officer**	**OA Officer Registration Authority Administrator**	**Security Compliance Auditor/Officer**
Default User Policy certificate	N/A	Security Officer Policy	Administrator Policy	Administrator Policy
Audit Logs				
View own logs		X	X	X
View all logs		X	X	X
Bulk & Report				
Process bulk files		X	X	
Create reports		X	X	X
Certificates				
Admin all categories		X	X	X
Admin selected categories				
Admin all types		X	X	X
Certification Authority				
Stop, Start and Maintain CA Services	X			
Recover Admin Service	X			
Backup and Restore CA databases				
View CA certificates		X	X	X
Update CA signing keys		X		

Privilege	**Trusted Roles**			
	OA Officer Master Users	**OA Officer Security Officer**	**OA Officer Registration Authority Administrator**	**Security Compliance Auditor/Officer**
Revoke CA keys		X		
View list of imported CAs		X		X
Import/Export CA public keys		X		
CA Subordinate				
View		X		X
Add subordinate CAs		X		
Revoke		X		
Directory				
Bind to Directory		X	X	
Change Directory password		X	X	
View entries		X	X	X
Create, Delete, Modify entries		X	X	
User Groups				
View		X	X	X
Rename		X		
Create		X		
Delete		X		
Admin all groups		X		X
Admin any group to which they belong			X	
License Information				
View		X	X	
Modify		X		
Policy OIDs				
Admin all OIDs		X	X	X
Queued Requests				

Privilege	**Trusted Roles**			
	OA Officer Master Users	**OA Officer Security Officer**	**OA Officer Registration Authority Administrator**	**Security Compliance Auditor/Officer**
View queued requests		X	X	X
Modify queued requests		X	X	
Create queued requests		X		
Delete queued requests		X		
Cancel queued requests		X		
Cancel request authorization		X		
Approve request authorization		X	X	
Roles				
View		X	X	X
Modify		X		
Create		X		
Delete		X		
Admin all roles		X		X
Admin selected roles			X[1]	
Searchbases				
View		X	X	X
Modify		X		
Create		X		
Delete		X		
Admin all searchbases		X	X	X
Security Policies				
View security policies		X	X	X
Modify security policies		X		

1 End-User Roles

Privilege	**Trusted Roles**			
	OA Officer Master Users	**OA Officer Security Officer**	**OA Officer Registration Authority Administrator**	**Security Compliance Auditor/Officer**
Export certificate specs.		X	X	X
Import certificate specs.		X		
Export user templates		X	X	X
Import user templates		X		
Force CRLs		X		
View CRLs		X	X	X
View user policies		X	X	X
Modify user policies		X		
Create user policies		X		
User Templates				
Admin all templates		X	X	X
Users				
View		X	X	X
Add		X	X	
Re-activate		X	X	
Deactivate/Remove		X	X	
Change DN		X	X	
Modify properties		X	X	
Revoke certificates		X	X	
Update key pairs		X	X	
Set for key recovery		X	X	
Cancel key recovery		X	X	
Modify key update options		X		
View activation codes		X	X	
Users – Advanced				

Privilege	**Trusted Roles**			
	OA Officer Master Users	**OA Officer Security Officer**	**OA Officer Registration Authority Administrator**	**Security Compliance Auditor/Officer**
Modify OIDs		X		
Change user's role		X		
Modify group membership		X	X	
Import new users		X		
Export to another CA		X		
Archive users		X		
View archived users		X		X
Retrieve archived users		X		
Restore information to Directory		X	X	
Perform PKIX requests		X	X	
Create user profile		X		
Recover user profile	X[2]	X		
Users – Other				
View attribute certificate		X	X	
Modify attribute certificate		X	X	
Create attribute certificate		X	X	X
Delete attribute certificate		X	X	
View registration password		X		
Modify registration password		X	X	
Validate registration password		X		
Notify client		X	X	
Modify Directory properties		X	X	

2 Master Users can setup Security Officers for recovery

5.2.4 Roles Requiring Separation of Duties

The GPO PA shall enforce separation of role for sensitive PKI functions by assigning the duties of OA Officer – Master User, OA Officer – Security Officer & Directory Administrator, OA Officer – Administrator, Security Compliance Auditor/Officer and OA System Administrator & Backup Operator (SABO) to separate individuals. No individual shall have more than one of these roles.

In addition, there is separation between personnel that create policies, implement policies, perform registration, and perform audits. To ensure that no one corrupt individual may modify the operation of the CA, all security sensitive functions shall require authorization by more than one individual.

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

The personnel holding GPO-PCA Trusted Roles are selected based on loyalty, trustworthiness, and integrity. All individuals filling Trusted Roles for the GPO-PCA must be U.S. citizens. NAC-I background checks are conducted that are suitably adjudicated in accordance with federal law. Copies of documentation proving an individual's citizenship and security clearance status (if applicable), for GPO-PCA Trusted Role personnel, will be maintained by the OA, and made available during compliance audits.

In addition to the above, individuals filling Trusted Roles for the GPO-PCA will:

- Have not knowingly been previously relieved of their PKI duties or responsibilities for reasons of negligence or non-performance of duties
- Are appointed in writing by the PA or OA as appropriate
- Have not knowingly been denied a security clearance, or had a security clearance revoked
- Have not been convicted of a felony offense
- That claimed education is accurate (last school that is claimed attended is checked)
- Have successfully completed an appropriate training program
- Have demonstrated the ability to perform their duties
- Are trustworthy

5.3.2 Background Check Procedures

Prospective employees for these Trusted Roles will be informed that personnel screening (e.g., references, credit checks, criminal record checks, etc.) will be conducted on any person that is being considered for such a position. All personnel that fill a GPO-PCA Trusted Role shall have a NAC-I background check conducted that is suitably adjudicated in accordance with federal law. The NAC_I check goes back at least five (5) years. The background check shall be refreshed every ten (10) years.

An active, current GPO security clearance (Secret, or Top Secret or above) may be used in lieu of the personnel screening identified above to establish that a NAC-I background check is conducted that is suitably adjudicated in accordance with federal law, since a GPO security clearance at the Secret, Top Secret or above level requires a full scope SSBI background investigation that meets and exceeds the NAC-I requirements, and to keep a GPO security clearance active requires that it be renewed (and another background check conducted) at least every five (5) years. Thus, an active GPO security clearance at the Secret, Top Secret or above level meets or exceeds the NAC-I background check requirements.

An active, current GPO security clearance may be used in lieu of the personnel screening identified above to establish that a NAC-I background check is conducted that is suitably adjudicated in accordance with federal law.

If the trustworthiness of an individual who fills a GPO-PCA Trusted Role is questioned while he or she is on the job, then the person will be removed from the sensitive position by the GPO Operational Authority while the problem is being investigated. The GPO OA shall provide a written record of the problem reported and the results of the investigation.

5.3.3 Training Requirements

Training has been established for each individual filling a Trusted Role for the GPO-PCA, including both the requirements and operations of the role and the PKI in general. An employee that has been assigned to a Trusted Role shall not begin working in that role until the person is trained for that role. The OA is responsible for ensuring that training is accomplished for employees that serve in Trusted Roles.

Training shall include the following areas:

- CA and RA security principles and mechanisms
- PKI software in use for the CA and RA
- All PKI duties the person shall perform for the role they are expected to perform
- Disaster recovery and business continuity
- Requirements of the Common Policy and this CPS

Records of the training that has been provided shall be maintained on site in paper or electronic media (e.g., a text document or a spreadsheet) and shall be made available to the auditors during every compliance audit.

5.3.4 Retraining Frequency and Requirements

Any significant change to this CPS, PKI hardware or software will require retraining of affected personnel. The OA will inform individuals filling Trusted Roles for the GPO-PCA when retraining is required, and will provide any required retraining. A written record of the retraining plan shall be created and maintained by the Operational Authority (OA).

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

Any person that operates in violation of the US federal PKI Common Policy or the GPO-PCA CPS or the practices and procedures stated herein, whether through negligence or with malicious intent, will have privileges revoked and may be subject to administrative and disciplinary action. Violations of this CPS that are determined by the GPO Operational Authority based on a fact based investigation to be due to malicious intent, shall subject to some form of administrative or disciplinary action, which shall be documented in writing by the GPO OA. Repeated or significant violation of this CPS or the Common Policy requirements shall result in privilege revocation and disciplinary action, which shall be documented in writing by the GPO OA. The range of disciplinary actions available will include termination.

5.3.7 Independent Contractor Requirements

Contractor personnel employed to perform functions pertaining to the GPO-PCA 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

All CA operators are provided appropriate system, application and cryptographic module documents which are retained at the CA location.

At a minimum, the following documentation will be supplied:

Role	Documentation Supplied
Master Users	• Safenet Luna documentation (from vendor) • Entrust Security Manager Operations Guide • FPKI Common Policy (CP) • PA approved CPS
System Administrator	• Windows 2000 on-line documentation (help files) • Entrust Security Manager Operations Guide • FPKI Common Policy (CP) • PA approved CPS
Security Officer	• Windows 2000 on-line documentation (help files) • Entrust Security Manager Operations Guide • Entrust Security Manager Administration Guide • Safenet Luna documentation (from vendor) • FPKI Common Policy (CP)

	• PA approved CPS
Registration Authority	• Entrust Security Manager Administration Guide • FPKI Common Policy (CP) • PA approved CPS

5.4 AUDIT LOGGING PROCEDURES

All security events on the CA's system are automatically recorded in audit log files. Such files are securely archived in accordance with the requirements of the US federal PKI Common Policy and this CPS.

As specified in the US federal PKI Common Policy, there are other auditable events that are not captured in electronic audit logs. These events, such as physical access events, are manually recorded in paper logs. The GPO-PCA OA is responsible for ensuring that all manual audit log events, as defined by the GPO PA and the compliance auditor are properly logged and the logs maintained as required.

5.4.1 Types of Events Recorded

All security auditing capabilities of the GPO-PCA operating system and CA applications required by the GPO CP and Common Policy Framework shall be enabled. As a result, most of the events identified in the table below shall be automatically recorded. 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)

The following table identifies additional audit events that are recorded:

Auditable Event	Method	Location

Auditable Event	Method	Location
SECURITY AUDIT		
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	Manually	CP or CPS change control
Any attempt to delete or modify the Audit logs	Automatically	OS logs
Obtaining a third party time stamp	Automatically	CA logs
IDENTIFICATION AND AUTHENTICATION		
Successful and unsuccessful attempts to assume a role	Automatically	CA logs
Change in the value of maximum authentication attempts	Automatically	CA logs
Maximum number of unsuccessful authentication attempts during user login	Automatically	CA logs
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	Automatically	CA logs
An Administrator changes the type of authenticator, e.g., from password to biometrics	Automatically	CA logs
KEY GENERATION		
Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)	Automatically	CA logs
PRIVATE KEY LOAD AND STORAGE		
The loading of Component private keys	Automatically	CA logs
All access to certificate subject private keys retained within the CA for key recovery purposes	Automatically	CA logs
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE		
All changes to the trusted public keys, including additions and deletions	Automatically	CA, OS logs[3]
SECRET KEY STORAGE		
The manual entry of secret keys used for authentication	Automatically	CA logs
PRIVATE KEY EXPORT		
The export of private keys (keys used for a single session or message are excluded)	Automatically	CA logs

3 Auditing of changes to trusted public keys can take place in various locations. These changes will be audited by the server OS or CA application (if performed through the CA).

Auditable Event	Method	Location
CERTIFICATE REGISTRATION		
All certificate requests	Manually	RA logs
CERTIFICATE REVOCATION		
All certificate revocation requests	Manually	RA logs
CERTIFICATE STATUS CHANGE APPROVAL		
The approval or rejection of a certificate status change request	Manually	RA logs
CA CONFIGURATION		
Any security-relevant changes to the configuration of the CA	Automatically	CA logs
ACCOUNT ADMINISTRATION		
Roles and users are added or deleted	Automatically	CA logs
The access control privileges of a user account or a role are modified	Automatically	CA logs
CERTIFICATE PROFILE MANAGEMENT		
All changes to the certificate profile	Automatically	CA logs
REVOCATION PROFILE MANAGEMENT		
All changes to the revocation profile	Automatically	CA logs
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT		
All changes to the certificate revocation list profile	Automatically	CA logs
LOCAL DATA ENTRY		
All security-relevant data that is entered in the system	Automatically	CA logs; OS logs
REMOTE DATA ENTRY		
All security-relevant messages that are received by the system	Automatically	CA logs; OS logs
DATA EXPORT AND OUTPUT		
All successful and unsuccessful requests for confidential and security-relevant information	Automatically	CA logs; OS logs
MISCELLANEOUS		
Installation of the Operating System	Automatically	OS logs
Installation of the CA	Automatically	CA, OS logs
Installing hardware cryptographic modules	Automatically	CA logs
Removing hardware cryptographic modules	Automatically	CA logs

Auditable Event	Method	Location
Destruction of cryptographic modules	Automatically	CA logs
System Startup	Automatically	OS logs
Logon Attempts to CA applications	Automatically	CA logs
Receipt of Hardware / Software	Manually	OA logs
Attempts to set passwords	Automatically	OS logs
Attempts to modify passwords	Automatically	OS logs
Backing up CA internal database	Automatically	CA logs
Restoring CA internal database	Automatically	CA logs
File manipulation (e.g., creation, renaming, moving)	Automatically	OS logs
Posting of any material to a repository	Automatically	CA, OS and Dir logs
Access to CA internal database	Automatically	CA logs
All certificate compromise notification requests	Manually	RA logs
Loading tokens with certificates	Automatically	CA logs
Shipment of Tokens	Manually	RA logs
Zeroizing tokens	Manually	RA logs
Re-key of the CA	Automatically	CA logs
Configuration changes to the CA server involving:		
Hardware	Manually	OA logs
Software	Manually	OA logs
Operating System	Manually	OA logs
Patches	Manually	OA logs
Security Profiles	Manually	OA logs
Appointment of an individual to a trusted role	Manually	OA logs
Designation of personnel for multiparty control	Manually	OA logs
PHYSICAL ACCESS / SITE SECURITY		
Personnel Access to room housing CA	Manually	OA logs
Access to the CA server	Manually	OA logs
Known or suspected violations of physical security	Manually	OA logs
ANOMALIES		
Software Error conditions	Automatically	CA logs
Software check integrity failures	Automatically	CA logs
Receipt of improper messages	Automatically	CA, OS logs

Auditable Event	Method	Location
Misrouted messages	Automatically	OS logs
Network attacks (suspected or confirmed)	Automatically	CA, OS logs
Equipment failure	Manually	OA logs
Electrical power outages	Manually	OA logs
Uninterruptible Power Supply (UPS) failure	Manually	OA logs
Obvious and significant network service or access failures	Manually	OA logs
Violations of Certificate Policy	Manually	PA logs
Violations of Certification Practice Statement	Manually	OA logs
Resetting Operating System clock	Automatically	OS logs

5.4.2 Frequency of Processing Log

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-PCA, 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-PCA, at least 70% of security audit data generated by the GPO-PCA since the last review shall be examined.

A Security Compliance Officer manually reviews the audit logs via the Entrust Security Manager Administration application, for policy violations or other significant events at least once per month.

The audit logs are made available during any compliance audits.

5.4.3 Retention Period for Audit Log

Audit logs shall be retained onsite until reviewed, in addition to being retained in the manner described below and archived as required in section 5.5. The individual who removes audit logs from the GPO-PCA system shall be an official different from the individuals who, in combination, command the GPO-PCA signature key.

The audit log data is kept live on the CA or RA hardware and archived as specified in the US federal PKI Common Policy.

The OA System Administrator & Backup Operator (SABO) is the personnel role that performs all functions related to the removal of audit log data from the system for storage on backup media. The OA SABO has no command authority in any way, even as part of a multi-party operation, of the GPO-PCA signature key.

5.4.4 Protection of Audit Log

Current physical logs (e.g., visitor sign-in logs) will be kept in the CA equipment location rooms. Only authorized personnel will have access to the physical log and only authorized personnel will make entries in physical log or other paper audit records.

The CA audit log is stored in regular operating system flat files. Each audit log file consists of an audit header, which contains information about the audits in the file and list of events. A Message Authentication Code (MAC) is created for each of the audit events and the audit log header. Each audit log file has a different audit key used to generate the MAC. The Entrust master key for the GPO-PCA is used to encrypt the audit key; the encrypted audit key is stored in the audit header.

The audit log can be spread across many files. A new audit log file is created when the current audit log file reaches a preset size of 1 Mbytes or the Entrust master key is updated.

The OA System Administrator & Backup Operator (SABO) is the only personnel role that has access to remove the security audit log data from the system by storing the data on backup media. This is controlled via the following:

- Operating system controls ensure that only the SABO can write or delete or copy the audit files.
- The SABO cannot access the PKI facility without a second authorized party (Security Officer, Master User or Registration Authority)
    - The SABO is ALWAYS required by the PKI facility physical access control system controls to be accompanied by AT LEAST one (1) other authorized person.
    - The physical security access control system ALWAYS enforces 2 person controls for the PKI room via the use of card key (GPO Employee ID badge) controls. Any person who is authorized by the GPO PKI Operational Authority to perform any PKI trusted role that is allowed to access the PKI Room has their GPO Employee ID badge programmed into the GPO Physical Access Security control system (Johnson Controls system).
        - Before any 2 people can gain physical access to the room housing the PKI systems, each person's badge must be swiped on the door reader and must exist as an authorized badge to be permitted entry to the PKI room.
    - 2 Party controls are ALWAYS required for any operation in which audit data is removed from the CA to be stored on backup and/or archive media.
- There is NO electronic access for the SABO to the CA system from outside of the physical computer console in the PKI Room which physically houses the CA system.

5.4.5 Audit Log Backup Procedures

The security audit data backup is archived by the OA System Administrator & Backup Operator (SABO) on a weekly basis. All files including the latest audit log file are copied to the off-site backup facility location via authenticated electronic data transfer. The audit logs backups are stored on secure storage at the off-site backup location which has physical security controls in compliance with this CPS. .

Paper based records and logs are PCAnned and digitized into PDF files and are backed up onto magnetic tape or digital media, and are also included in the archive records stored in the secure archive facility. The Security Officer and the SABO perform the PCAnning of the paper based records and the storage of the PDF digital files onto the archive media. Paper based records which are PCAnned and archived include: the PKI Room paper physical access logs, Audit summary logs and Physical Access Review Logs.

The secure archive facility is off-site from the facility in which the primary PKI systems are located and operate. The GPO-PCA uses the Iron Mountain commercial facility for off-site archive storage. The Iron Mountain facility is guarded and monitored 24 hours per day, 7 days per week, 52 weeks per year for unauthorized access.

5.4.6 Audit Log Collection System (Internal vs. External)

The CA audit system is internal to the Entrust Authority Security Manager software. The CA audit system is automatically invoked at CA system startup, and cease only at CA system shutdown. If it is determined that the automated CA audit system has failed and is not operational, CA operations shall be suspended until the audit system failure has been resolved. The GPO PA shall determine whether to resume operations after such an audit system failure.

The CA audit system is configured such that security audit data is protected against loss. The Entrust COTS CA software is configured by the GPO-PCA OA to provide this protection. This COTS software ensures that a new audit log file is created to prevent the possibility of overwriting or overflow of the automated CA log files.

5.4.7 Notification to Event-Causing Subject

The US federal PKI Common Policy imposes no requirement to notify a Subject that an event was audited therefore this CPS does not require notification to a Subject that an event was audited.

5.4.8 Vulnerability Assessments

The GPO-PCA OA and the Security Auditor trusted role staff shall be watchful for anomalies and attempts to violate the integrity of the system, including the equipment, its physical location, and its personnel. The OA will, as part of its regular security audit review, look for events such

as repeated failed actions, requests for privileged information, attempted access of system files, unauthenticated responses, and continuity of security audit data.

Periodic monthly Vulnerability assessments using commercial off the shelf (COTS) software, such as McAfee Foundstone or ISS Internet PCAnner or equivalent, shall be executed by the OA against all GPO-PCA systems, including the Directory systems and CSS, to ensure that the integrity of the systems has not been violated. In addition, weekly reviews of the CA logs (Entrust COTS software) and Operating System logs are conducted by the PKI Security auditor.

Suspicious activity will be reported to the GPO PA and the OA.

5.5 RECORDS ARCHIVAL

5.5.1 Types of Events Archived

The following table identifies the archive records that are retained:

Archive Records
CA accreditation (if applicable)
Certification Practice Statement
Contractual obligations
System and equipment configuration
Modifications and updates to system or configuration
Certificate requests
Revocation requests
Subscriber identity Authentication data
Documentation of receipt and acceptance of certificates
Documentation of receipt of tokens
All certificates issued or published
Record of CA Re-key
All information on ARLs and CRLs issued and/or published
All Audit Logs
Other data or applications to verify archive contents
Certificate Policy
Other agreements concerning operations of the CA
Subscriber agreements
Subscriber encryption-decryption key pairs

Archive Records
Documentation of receipt of tokens
All certificates issued or published
Record of CA Re-key
All CRLs issued and/or published
Other data or applications to verify archive contents
Compliance Auditor reports
Any changes to the Audit parameters, e.g., audit frequency, type of event audited
Any attempt to delete or modify the Audit logs
Whenever the CA generates a key (Not mandatory for single session or one-time use symmetric keys)
All access to certificate subject private keys retained within the CA for key recovery purposes
The approval or rejection of a certificate status change request
Appointment of an individual to a Trusted Role
Destruction of cryptographic modules
All certificate compromise notifications
Remedial action taken as a result of violations of physical security
Violations of Certificate Policy
Violations of the Certificate Practice Statement

5.5.2 Retention Period for Archive

Archive data must be retained for a minimum of 10 years and 6 months. Archive records are kept as specified in the US federal PKI Common Policy. Applications required to process the archive data will also be maintained for the archive retention period. The GPO-PCA OA is responsible for knowing where the archived material is, and for ensuring that it is not lost during reorganizations, physical organization moves, and so on. Media are used that can reliably store the archive data for the required minimum retention period. These media are hard drives and CD's that reliably meet the required retention period.

Archive records that have been kept for 20 years are transferred to a GPO PA approved archive facility for indefinite storage.

5.5.3 Protection of Archive

When possible the archive data will be digitally signed by the GPO-PCA. This will provide an integrity check that can be used to verify that the data has not been modified.

Long-term archive data for the GPO-PCA will be recorded on read-only media and stored off-site in a fireproof safe/vault with locks. Short-term media will be stored in a location separate from the CA equipment. The archive media is protected by physical security in that it is retained in a restricted access location to which only the GPO PA and GPO-PCA OA have access. This location will adhere to the physical security practices defined in this CPS.

The archives will be labeled with the CA DN and the date.

A list of authorized individuals that have the permissions necessary to access and delete the on-line archive files will be maintained at the CA site, and all accesses will be recorded. These records will be made available to the auditors during compliance audits.

5.5.4 Archive Backup Procedures

Archive files are backed up along with the security audit logs.

Paper archives may be backed up to microfiche, or other long-term storage solution, as directed by the PA.

5.5.5 Requirements for Time-Stamping of Records

Time-stamping of records is accomplished via the CA system, using the CA system clock. The CA system clock is synchronized on a periodic basis with the NIST official time source, using the IETF standard Network Time Protocol (NTP), to ensure that the CA system clock is accurate. The SABO and the Security Officer ensure that the NTP service is operational on the CA system. The NTP service is set for automatic service startup on the CA system to ensure that the NTP service is always started whenever the CA sysem must be started.

5.5.6 Archive Collection System (Internal and External)

GPO-PCA archive data will be collected as part of the routine system backup procedures, along with directory shadowing, and explicit file copies of GPO-PCA files that do not reside in the underlying GPO-PCA database. Paper based CA records that are required for archive will be copied or digitally PCAnned, and packaged by the Operational Authority for transmittal to the archive site. The Operational Authority shall verify that all required archive records are contained in packages that are transmitted and moved to the archive facility.

5.5.7 Procedures to Obtain and Verify Archive Information

The archive system automatically verifies the archive media immediately after archive creation.

The OA is responsible for ensuring that all request for archive information come from an authorized source. The archive condition is verified during every compliance audit.

5.6 KEY CHANGEOVER

The Subscriber certificates issued by the GPO-PCA are set up for automatic key roll-over. As such, the encryption and digital signature key pairs of the Subscriber are automatically updated prior to expiry. Following CA key changeover, the new CA key will be used to CRLs and certificates going forward. Following CA key changeover, the new CA key only will be used to sign CRLs and certificates going forward. The new CA key shall comply with the validity period requirements in section 6.3.2 of this CPS, and the GPO CP and Federal PKI Common Policy CP. The GPO-PCA uses key rollover certificates using the facilities of the Entrust COTS PKI software (which is FIPS certified) to accomplish CA key changeover. The old CA key is held and protected using the same mechanisms as the new CA key, which utilize the Safenet LunaSA HSM (which is FIPS certified to Level 3) and the Entrust COTS PKI software. The GPO PKI and GPO-PCA shall continue to interoperate with the Common Policy Root CA after the

Common Policy Root CA performs a key rollover, whether or not the DN of the Common Policy Root CA is changed. The Entrust COTS PKI software allows this to be accomplished. In the event that the Federal Bridge CA (FBCA) performs a CA key rollover, the GPO-SCA shall continue to interoperate with the FBCA after the FBCA performs a key rollover, whether or not the FBCA DN is changed.

The GPO PKI and GPO-PCA shall continue to interoperate with the Common Policy Root CA after the Common Policy Root CA performs a key rollover, whether or not the DN of the Common Policy Root CA is changed. The Entrust COTS PKI software allows this to be accomplished.

5.7 COMPROMISE AND DISASTER RECOVERY

The PA and OA maintain a GPO PKI Contingency Plan, which is updated periodically (at least on an annual basis) or as major system changes dictate, to define how the PKI is restored to service in a reasonably timely manner and in accordance with this CPS and CP requirements in the event of a failure. The GPO PKI Contingency Plan shall define the acceptable system outage and recovery time periods.

In any key compromise situation, a report will be filed with the PA indicating the circumstances under which the compromise occurred. The PA will determine if a possible follow up investigation and potential action is required.

5.7.1 Incident and Compromise Handling Procedures

The GPO Computer Security Incident Response Team (CSIRT) Procedures shall be used by the GPO PA and GPO OA when handling incidents or compromise events. These procedures are included in this CPS by reference.

These procedures include the following steps:

- Report and document the incident (by using the GPO IT Help Desk ticketing system) (All steps for responding to the incident in the following steps will be documented also)
- Identify the nature and scope of the incident
- Notification of the incident and its associated potential impacts and affects to stakeholders (Federal PKIPA, Subscribers, PA, OA, and Relying Parties)
- Protecting Evidence and Logs
- Containment of the results and affects of the incident to reduce adverse impacts
- Eradication of the causes and sources of the incident and any adverse results
- Recovery to restore the GPO-PCA to effective and efficient operations

- Follow-up to notify stakeholders (Federal PKIPA, Subscribers, GPO PA, GPO OA and Relying parties) of the results of the recovery from the incident and GPO-PCA operational status
- Post-incident review to ensure lessons learned are incorporated into future operations and practices

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

In the event of an inoperative GPO-PCA due to equipment damage, software or Operating System failure, or data corruption, where all copies of the CA signature keys are **not** destroyed, the following steps, at a minimum, are taken to recover a secure environment:

- The GPO-PCA infrastructure (hardware and software) will be re-built and/or restored from backup as necessary
- The GPO-PCA shall be reconstituted within 72 hours, in the event of a catastrophic failure
- The directory data, encryption certificates and CRLs/ARLs, are restored if the directory becomes unusable and must be restored from backup or if the directory is suspected to be corrupt.

5.7.3 Entity (CA) Private Key Compromise Procedures

In the event of an inoperative GPO-PCA, where all copies of the GPO-PCA signature keys are **not** destroyed, the following steps, at a minimum, are taken to recover a secure environment:

- The GPO-PCA infrastructure (hardware and software) will be re-built and/or restored from backup as necessary
- The directory data, encryption certificates and CRLs/ARLs, are restored if the directory becomes unusable and must be restored from backup or if the directory is suspected to be corrupt
- The GPO Policy Authority and Federal PKI Policy Authority shall be informedGPO-PCA in the event that the CA cannot issue a CRL within 72 hours after the time specified in the next update field of its currently valid CRL

5.7.3.1 CA Signature Keys are Compromised

In the event of the compromise of the GPO-PCA private key, the federal PKI PA will be informed via secure communication from the OA. The CA installation shall be reestablished in accordance with any instructions and direction from the federal PKI PA. In general, the OA will revoke the certificates for the GPO-PCA, install a new GPO-PCA, work with the Federal PKI Policy Authority to obtain a new GPO-PCA certificate, and publish the new GPO-PCA certificate to the directory. The OA shall review all MOA's that exist and make determination of any other entities, Policy Authorities or CA's that need to be notified and notify all affected entities, Policy Authorities or CA's.

The OA will notify the Subscribers of the GPO-PCA of the key compromise via a secure communication. The Subscriber certificates will be renewed automatically by the GPO-PCA under the new CA key pair, using the capabilities of the CA software. The fingerprint of the new GPO-PCA key pair will be placed onto the GPO PKI web site (http://www.gpo.gov/projects/pki.htm) and all Subscribers instructed by email from the GPO PKI service that this fingerprint can be validated as a backup method to ensure that the proper new CA key is installed.

5.7.3.2 Secure Facility Impaired After a Natural or Other Type of Disaster

In the event of a disaster of the GPO-PCA when the GPO-PCA private key is not compromised and is available, the following steps, as a minimum, are taken to recover a secure environment:

- The GPO-PCA infrastructure (hardware and software) will be re-built at an alternate facility
- The directory data, encryption certificates and CRLs/ARLs, are restored to the directory
- In the event that the disaster results in all copies of the CA keys being destroyed, the GPO Policy Authority (PA) shall be notified at the earliest feasible time, and the Federal PKI PA shall be notified as well

5.7.3.3 Notification Requirements for Disaster Recovery, Compromise and Incidents

The Federal PKI Policy Authority and the GPO PA shall be notified by the GPO-PCA OA if the GPO-PCA experiences any of the following:

- Suspected or detected compromise of the GPO-PCA
- Suspected or detected compromise of a CSS (OCSP) server
- Physical or electronic penetration of the GPO-PCA
- Successful denial of service attacks on GPO-PCA components
- Any incident preventing the CA from issuing a CRL within 48 hours of the issuance of the previous CRL.

The GPO-PCA OA shall reestablish operational capabilities of the GPO-PCA as quickly as possible, in accordance with the procedures and requirements of this CPS.

5.7.4 Business Continuity Capabilities after a Disaster

The GPO-PCA has an off-site backup location so that the GPO-PCA shall be recovered and made operational within 24 hours of a failure of the primary GPO-PCA system.

5.8 CA OR RA TERMINATION

In the event that the GPO-PCA ceases operation or is otherwise terminated:

- All Subscribers and Relying Parties must be promptly notified of the cessation
- All Subscribers will be notified of cessation using email communication, if email is available
- All certificates issued by the GPO-PCA shall be revoked no later than the time of cessation (any CRL issued must be valid until 30 days after the last certificate issued by the GPO-PCA expires)
- All current and archived GPO-PCA identity proofing, certificate, validation, revocation/suspension, renewal, policy and practices, billing, and audit data shall be sent to the GPO PA archive facility

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

Safenet LunaSA hardware tokens (validated for FIPS 140 Security Level 3) will be used to generate and store the GPO-PCA CA keys. GPO-PCA key pair generation will be performed in accordance with a written Key Generation script (procedure) which must create a verifiable audit trail that the security requirements for procedures were followed. The audit trail must identify and document any failures or anomalies in the key generation process, and any corrective actions taken. The documentation of the procedure must be detailed enough to show that appropriate role separation was used.

The CA key pair generation will be in compliance with PKCS#1, including the tests for primality. The private key will never be exposed outside the module in unencrypted form.

6.1.1.2 Subscriber Key Pair Generation

Entrust software will initiate the process of generating the key pairs for the GPO-PCA Subscriber. Use of Federal Information Processing System (FIPS) approved cryptographic modules precludes exposure of plaintext key outside of the cryptographic modules. The GPO-PCA Subscriber's signature key pair will be generated on a FIPS 140 Level 1 or higher (the RA will be generated on a Level 2 hardware token), validated cryptographic module and the Subscriber's public signature key is delivered to the CA at that time, and the Subscriber's encryption key pair will be generated at the CA machine and the Subscriber's private decryption key will be delivered to the Subscriber at that time. For subscribers that have keys issued on hardware tokens, an authorized GPO PKI Trusted Role staff member (Security Officer or Registration Authority) shall issue the token to the subscriber.

Subscriber's signature keys shall be generated by the Subscriber (the client software or hardware being used by the Subscriber) and the encryption keys shall be generated by the CA. Both software and hardware may be used, as specified in Section 6.2.1. Any pseudo-random numbers used for key generation material shall be generated by a FIPS approved module. The Entrust COTS client software meets all FIPS requirements and is a FIPS approved module at Level 1. The CA uses the Entrust COTS software, which uses a FIPS approved module, and also uses the Safenet LunaSA hardware cryptographic module, which is also a FIPS approved module.

6.1.1.3 Certificate Status Server (CSS) Key Pair Generation

Safenet LunaSA hardware token (validated for FIPS 140 Security Level 3) will be used to generate and store the cryptographic key for the CSS system.

6.1.2 Private Key Delivery to Subscriber

Private signature keys will be generated and remain within the crypto boundary of the cryptographic module of the key owner, thus no delivery is required.

Private decryption keys will be delivered by the GPO-PCA using the security protection provided by PKIX-CMP and shall use a cryptographic algorithms in the PKIX-CMP that are as strong or stronger than the 2048 bit RSA public/private key pairs. The GPO Operational Authority uses the Entrust COTS software capabilities for PKIX-CMP, which provides strong encryption algorithms and key sizes that are as strong or stronger than the 2048 bit RSA public/private key pairs used by the GPO-PCA, to protect these RSA private decryption keys.

6.1.3 Public Key Delivery to Certificate Issuer

Public keys are delivered to the certificate issuer electronically in a certificate request in accordance with PKIX-CMP protocol. The Entrust COTS PKI software is used by the GPO-PCA for its Subscribers to provide appropriate encryption and integrity cryptographic mechanisms in compliance with the PKIX-CMP protocol, which are cryptographically as strong or stronger than the 2048 bit RSA public keys that are requested for certification. All GPO-PCA Subscribers are required to use the Entrust PKI COTS software.

6.1.4 CA Public Key Delivery to Relying Parties

GPO-PCA certificates shall be posted in the border directory, so Entity CAs have access. The border directory shall implement access controls sufficient to prevent a certificate substitution attack. When a CA key rollover is accomplished, the GPO-PCA shall issue a key rollover certificate, which the Entrust COTS PKI software shall automatically make available in the GPO border directory. The trust anchor certificate is provided to Subscribers on a CD at the time of Subscriber in-person identity proofing.

6.1.5 Key Sizes

The GPO-PCA use of Secure Socket Layer (SSL), or TLS, or another protocol providing similar security to accomplish any of the requirements of the federal PKI Common Policy CP shall require at a minimum AES (12b bits) or equivalent for the symmetric key, and at least 2048 bit RSA or equivalent for the asymmetric keys. Use of SSL or TLS or another protocol providing similar security after 12/31/2030 shall require at a minimum AES (128 bits) or equivalent for the symmetric key, and at least 3072 bits RSA or equivalent for the asymmetric key. Public keys in all self-signed certificates generated after 12/31/2010 that expire after 12/31/2030 shall be at least 3072 bits for RSA, or at least 256 bits for ECDSA.

The GPO-PCA key modulus shall comply with this CPS.

Subscriber’s key modulus is 2048 bits for RSA.

The GPO-PCA uses AES-256 for database encryption.

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

sha-256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

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

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}

6.1.6 Public Key Parameters Generation and Quality Checking

Public key parameters shall always be generated and checked in accordance with the standard that defines the cryptographic algorithm in which the parameters are to be used. Parameter quality checking (including primarily testing for prime numbers) shall be performed in accordance with FIPS 186-2.

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

Keys are certified for use in signing, non-repudiation or encrypting. Public keys that are bound to human subscribers shall be used only for signing or encrypting, but not both. Subscriber certificates used for digital signatures will set the *digitalSignature* bit and the *nonRepudiation* bit (except for Device certificates). Device certificates issued will not have the *nonRepudiation* bit set. Certificates to be used for data encryption set the *keyEncipherment* bit. GPO-PCA certificates shall set two key usage bits: *cRLSign* and *CertSign*. All certificates issued by the GPO-PCA shall have a critical key usage extension, in accordance with the Federal PKI Common Policy Framework.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

The relevant standard for cryptographic modules is the latest version of the FIPS 140 series, *Security Requirements for Cryptographic Modules*.

In accordance with FIPS 201, the relevant NIST Guideline for PIV Card Issuers (PCI) is NIST SP 800-79, *Guidelines for the Accreditation of Personal Identity Verification Card Issuers*, which utilizes various aspects of NIST SP 800-37 and applies them to accrediting the reliability of PCIs.

The CA shall use a hardware cryptographic module that is validated to FIPS 140 Security Level 3 (or higher). The CA has a hardware cryptographic module for operations that meets this requirement.

The RA's shall use a hardware cryptographic module that is validated to FIPS 140 Security Level 2 (or higher). RA's are supplied a hardware cryptographic module that meets this requirement for use with the CA and this CPS. The Safenet token and associated cryptographic module used by the GPO-PCA for this function meets this requirement.

PIV Cards are PKI tokens that have private keys associated with certificates asserting id-fpki-common-authentication or id-fpki-common-cardAuth. PIV Cards shall only be issued using card stock that has been tested and approved by the FIPS 201/FICAM Testing Program and listed on the GSA Approved Products List (APL). On an annual basis, for each PCI configuration used (as defined by the FIPS 201/FICAM Testing Program), one populated, representative sample PIV Card shall be submitted to the FIPS 201/FICAM Testing Program for testing.

The GPO-PCA Subscribers that have a certificate that asserts any of the OIDs permitted by this CPS shall use either a hardware or software cryptographic module that is validated to FIPS 140 Security Level 1 (or higher). The Entrust COTS client software used by the GPO-PCA meets this requirement.

GPO-PCA Subscribers that have a certificate that asserts the Federal PKI Common Policy OID for id-fpki-common-hardware, or the OID for fpki-common-authentication, or the OID for fpki-common-cardAuth, or GPO Medium-Hardware, GPO Authentication, or GPO CardAuth shall use a cryptographic module that is validated to FIPS 140 Security Level 2 (or higher). The Safenet token and its associated cryptographic module used by the GPO-PCA for this purpose meet this requirement.

All cryptographic modules permitted by this CPS shall operate such that the private asymmetric cryptographic keys are never output in plaintext (unencrypted). The Entrust COTS software and Safenet hardware tokens used by the GPO-PCA meet this requirement.

The Certificate Status Server (OCSP system) shall use a cryptographic module certified to FIPS 140 Level 2 or higher. The Corestreet CSS/OCSP system is used by the GPO-PCA in conjunction with the Safenet hardware cryptographic module to meet this requirement.

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

Multi-person control requires that more than one individual independently authenticate themselves to the system that will perform CA operations. This mechanism prevents any single party (CA or otherwise) from gaining access to the certificate-signing key.

The CAs private signing key, and any backup copies, are generated and stored on a hardware security module (HSM). The HSM enforces multi-person access control for the CA.

The LunaSA PED Keys are used to initialize and login to the LunaSA hardware tokens, to create clones and to enforce multi-person (M-of-N) controls. The following paragraphs describe the various PED keys and their intended uses:

Gray PED Key - The Gray PED Key is the default key used to initialize and potentially re-initialize the LunaSA Token. Any Gray PED Key can be used to initialize or re-initialize any Token. There will be a total of 3 Gray PED Keys. Once the key generation ceremony is complete the 3 Gray PED Keys will be secured with tamper-evident seals and securely stored by the OA.

Blue PED Key - The Luna Security Officer (LSO) PED Key is used to clone Tokens. The LSO PED Key holds the LSO PIN and is used for creating Token users and changing Token passwords. There will be a total of 3 Blue PED Keys. Once the key generation ceremony is complete, the Blue PED Keys will be secured with tamper-evident seals and securely stored by the OA.

Black PED Key - The Black PED Key is used to login to the Luna Token when starting Entrust/Authority. There will be 3 Black PED Keys. Once the key generation ceremony is complete, one Black PED Key will be held in the possession of the Luna User; the other Black PED keys will be secured with tamper-evident seals and securely stored by the OA.

Red PED Key - The Red Key, Cloning PED Key, is used to clone LunaSA tokens. It carries the domain identifier for the Tokens. It is created/imprinted with the first Token and then carries the domain to the other Tokens thus permitting PED Key cloning amongst only those Tokens. There will be 3 Red PED Keys. Once the key generation ceremony is complete, the 3 Red PED Keys will be secured with tamper-evident seals and securely stored by the OA.

Green PED Key - The Green PED keys are used for M of N capabilities. M of N is an optional access-restriction function to further enhance the security of LunaSA token operations. M of N involves an additional password or PIN, applied to the token, which must accompany the User or LSO login keys. The M of N password is a shared secret that is distributed (or split) among several Green PED keys. M of N will be 1 of 3. The shared secret will be split amongst 3 Green PED keys. There will be 1 Green PED key required at each login. Any future login to the token requires that 1 of the 3 green share keys be provided, in addition to either the blue LSO key or the black Luna User key. Once the key generation ceremony is complete 2 sets of 3 Green PED Keys will be secured with tamper-evident seals and securely stored by the OA. The 3 remaining Green PED keys will be distributed to the appropriate individuals.

The OA maintains a list of personnel that have been given access to the PED keys. The list will be made available for inspection during compliance audits.

6.2.3 Private Key Escrow

Under no circumstances are signature keys used to support non-repudiation or digital signature services escrowed by a third party.

The GPO-PCA escrows all private key management encryption keys.

6.2.3.1 Escrow of CA Encryption Keys

The CA keys shall not be escrowed.

6.2.4 Private Key Backup

The HSM containing the GPO-PCA keys will be cloned in order to support the high availability CA configuration and Disaster Recovery. Cloning copies the contents of one secure cryptographic token to another without exposing the keys outside of the HSM. The cloning procedure maintains hardware secured backups and verifiable audits through a direct hardware-to-hardware backup procedure. To prevent unauthorized use of backup materials, backup tokens maintain the same access controls as the original.

The token will be cloned 2 times to create 3 identical tokens (1 production, 1 production backup and 1 off-site backup) of the CA keys. The initial cloning procedure will be performed as part of the key generation ceremony.

The OA periodically tests all tokens, including the clones, to ensure that they are operational. Tokens that have failed will be immediately replaced by new clones.

6.2.4.1 Backup of GPO-PCA Private Signature Key

The GPO-PCA private signature keys are backed up under the same multi-person control as the creation of the original signature key. This backup/cloning procedure is completed as a formal script that specifies the detailed step-by-step procedure. The script defines the individuals that are required to complete the backup/cloning procedure and meet the multi-person control requirement.

A single copy of the signature key is securely stored at the GPO-PCA location. A second copy will be securely stored at an off-site backup location. Copies of the signature key shall be stored on cryptographic tokens and shall be placed in secure containers, and the activation information for the signature key shall be placed in a separate security container, in tamper-evident envelopes, from the cryptographic tokens.

6.2.4.2 Backup of Subscriber Private Signature Key

Subscriber private signature keys for any Medium Hardware assurance certificate issued under this CPS, shall not backed up, escrowed, copied or archived.

For Medium Assurance certificates, the Subscriber private signature keys may be backed up or copied, but must be held in the Subscriber’s control. The Entrust COTS software provides the capabilities to meet these requirements.

6.2.4.3 Backup of Subscriber Private Key Management Key

Backed up Subscriber private key management key shall not be stored in plaintext outside of the cryptographic module. The Entrust COTS and Safenet hardware tokens provide the cryptographic module capabilities to meet these requirements.

6.2.4.4 Backup of Certificate Status Server (CSS) Private Key

The CSS Private key shall be cloned using the HSM in order to support high availability and support the off-site backup location for disaster recovery. The cloning procedure maintains hardware secure backup and verifiable audits through a direct hardware-to-hardware backup procedure using the HSM. The cloning token shall be stored in a secure container. To prevent unauthorized use of the backup materials, the cloning token is stored in a secure container that is located in the same physical location and has the same physical access controls as the production HSM.

6.2.5 Private Key Archival

. The CA private signature key shall not be archived. The CA private signature key is stored inside the LunaSA hardware token (FIPS 140 certified at Security Level 3) and no backup CA key storage tokens are ever sent to the secure archive facility. This is accomplished by the procedures used for the archive, in that a specific step in this procedure states that in no case is a GPO-PCA backup LunaSA key storage token to be archived.

Subscriber private signature keys shall not be archived.

CSS private signature keys shall not be archived.

The GPO-PCA uses the Entrust COTS CA software to escrow key management keys for Subscribers to enable key recovery, and the protocols and cryptographic methods of the Entrust COTS CA software are used for this purpose. Entrust COTS CA software uses cryptographic parameters, including AES-256 symmetric key encryption for CA database encryption, which are as strong or stronger than the key management keys being protected.

6.2.6 Private Key Entry into or from a Cryptographic Module

Private keys are generated within the cryptographic module. Use of FIPS 140 validated cryptographic modules prevents exposure of unencrypted key outside the cryptographic modules.

6.2.7 Private Key Storage on a Cryptographic Module

See section 6.2.1 for this information.

6.2.8 Method of Activating Private Key

The CA cryptographic module retrieves and activates the CA private signing key only when needed. The GPO-PCA private signing key is never exposed outside of the cryptographic module. Activation of the GPO-PCA private signature key requires the Black or Blue PED Key and the associated PIN, in addition to one Green PED Key.

The Subscriber is authenticated to the cryptographic module before the activation of the private key associated with certificates issued by this CA under id-fpki-common-authentication, id-fpki-common-policy, id-fpki-common-hardware and id-fpki-common-devices. Methods of authentication include but are not limited to passphrases, PINs or biometrics. Entry of activation data is protected from disclosure (i.e., the data is not displayed while it is entered). For certificates issued under id-fpki-common-cardAuth, Subscriber activation is not required to use the associated private key.

Subscriber private keys are activated when the Subscriber logs into (i.e. authenticates to) the certificate application.

6.2.8.1 Access to Activated Cryptographic Modules and Private Key

Cryptographic modules and private keys that have been activated shall not be available to unauthorized access. For the CA and CSS (OCSP) systems, this is accomplished via the physical security controls described above in section 5.1 (and all its subsections) of this CPS. For RA's this is accomplished via the RA obligations described above in this CPS in section 2.1.2. The RA is required to ensure that the cryptographic module is not left unattended when the private key has been activated. In addition, the inactivity timer for the RA software and token (the Entrust COTS software and Safenet token) shall be set to 15 minutes to provide technical preventative control to limit the risks of unauthorized access to the activated private key. Subscribers are required by the obligations described above in this CPS in section 2.1.3 to ensure that the cryptographic module is not left unattended when the private key has been activated and before the private key has been deactivated. In addition, the inactivity timer for the Subscriber software configured in the Entrust COTS software is set to 15 minutes to provide a technical preventative control to limit the risks of unauthorized access to the activated private key.

6.2.8.2 Access to CA Cryptographic Modules When Not in Use

CA cryptographic modules shall be stored in a secure container (safe) when the module is not in active use with the CA application. The backup tokens used for cloning the CA keys for disaster recovery and high availability purposes shall be stored in a secure container (safe) when not in use for purposes of authorized key recovery or backup operations. The GPO primary site and the off-site backup location have security containers for this purpose.

6.2.9 Method of Deactivating Private Key

The private keys remain active for the period of login. The login period is ended either by the Subscriber logging out from the certificate application or automatically as determined by a preset timer. For GPO-PCA Subscribers, the idle-timer is set to 15 minutes.

For those Subscribers using a hardware cryptographic token, the Subscriber's token will be deactivated as described above or by removing the token from the reader.

6.2.10 Method of Private Key Destruction

Individuals in trusted roles shall destroy CA, RA and CSS (OCSP) private signature keys when they are no longer needed. The methods of private key destruction are described below.

When the CA private key is to be destroyed, which is only under the conditions that the key is no longer needed and the certificates which correspond to it are expired or revoked, this shall be performed using the LunaSA token zeroize command in accordance with the LunaSA documentation. This shall be a scripted event with a written script. The command shall be repeated to ensure that the private key is destroyed. The LunaSA hardware shall be retained in storage in safe #2 in the PKI Room, in this event.

When the CSS (OCSP) private signature key is no longer needed and can be destroyed, the vendor supplied commands shall be used in conjunction with the vendor hardware to zeroize the private signature key that is not needed, using the Corestreet documentation.

When an RA private signature key is no longer needed and can be destroyed, the vendor supplied command to zeroize that key shall be used using the vendor supplied documentation from Safenet or appropriate vendor token.

Subscribers shall either surrender their cryptographic module to authorized CA or RA personnel for private signature key destruction once that signature key is no longer needed (when the certificate associated with the private key has expired or has been revoked), or shall use the vendor supplied command (using the Entrust COTS software for software stored certificates or the Safenet token commands for hardware stored keys) to destroy the private signature key. For Subscriber private keys that are stored on a hardware token, the vendor supplied software command to re-initialize and zeroize the token shall be used, following the documentation of the vendor (Safenet)

6.2.11 Cryptographic Module Rating

The GPO-PCA cryptographic module is rated at FIPS 140 Security Level 3. The rating for the cryptographic module used by the CSS is FIPS 140 Security Level 3. The rating for the cryptographic module used by RA and LRA personnel is FIPS 140 Security Level 2.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

The public keys are archived as part of the certificate archival.

6.3.2 Certificate Operational Periods and Key Usage Periods

The GPO-PCA key pairs are set up for manual update. The GPO-PCA key validity period is as follows:

Key Type	Key Validity Period	Certificate Validity Period
Signature	3 years	7 years

The key validity periods for the GPO SSP CSS (OCSP) key pair is as follows:

Key Type	Key Validity Period	Certificate Validity Period
Signature	3 years	3 years

The key validity periods for GPO-PCA Subscribers are as follows:

Key Type	Maximum Private Key Validity Period	Maximum Certificate Validity Period
Encryption/Key Management	Not Applicable	2 years
Signature or Non-Repudiation	90% Certificate Lifetime	3 years
Card Authentication (Common Policy and GPO Policy)	3 years	3 years
PIV Authentication and GPO Authentication	3 years	3 years

Device (GPO Policy and Common Policy)	3 years	3 years

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

Activation data (biometrics, password or PIN) will be used to protect access to use of a private key. Password-type activation data (i.e. not biometric or PIN) used by the RA's is required to meet the following criteria:

- At least eight characters
- At least one numeric character
- At least one uppercase character
- At least one lowercase character
- At least one special character
- No repetition of the previous 12 passwords

Password-type activation data (i.e. not biometric or PIN) used by the Subscribers is required to meet the following criteria:

- At least eight characters
- At least one numeric character
- At least one uppercase character
- At least one lowercase character
- No repetition of the previous 3 passwords

Subscriber and RA activation data is not transmitted electronically to the subscriber or the RA, respectively.

PIN-type activation data is required to be between 4 to 8 digits in length, inclusive.

Biometric-type activation data is dependent on the manufacturer and type of biometric system in use.

CA activation data shall not be transmitted electronically over a network, and shall be controlled in accordance with CA Key Generation Ceremony documentation, which is maintained by the Policy Authority.

6.4.2 Activation Data Protection

Activation data for RA's and Subscribers is not to be written down. However, if activation data is written down, it will be secured at the level of the data that the associated cryptographic module is used to protect, and will not be stored with the cryptographic module.

Activation data will never be shared.

6.4.3 Other Aspects of Activation Data

Procedures followed to change PED Key PINs are described in the LunaSA documentation.

6.5 COMPUTER SECURITY CONTROLS

The CA server instantiation is tightly controlled and audited as part of the key generation ceremony. All software loaded on the CA server is from original manufacturer distribution media.

The GPO-PCA server is built on Windows 2003 Server operating system (with the current Service Pack). The Windows 2003 Server operating system will have the following security features enabled: identification and authentication for all users, discretionary access control, and security audit. The Windows 2003 Server operating system is designed and configured to provide self-protection and process isolation.

The GPO-PCA server operates with the minimal number of local accounts required. No one will be able to perform remote login. The GPO-PCA will only run the network services required to operate the CA.

6.5.1 Specific Computer Security Technical Requirements

The operating system requires authenticated logins, provides discretionary access control, audit capability, enforces domain integrity boundaries, and supports recovery from key subsystem or system failure.

The CA Software is validated FIPS 140-2 level 1 and the HSM is validated FIPS 140-2 level 3, they provide the following security technical controls:

- Require authenticated logins
- Provide Discretionary Access Control
- Provide a security audit capability
- Restrict access control to GPO-PCA 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-PCA random access memory
- Require use of cryptography for session communication and database security
- Archive GPO-PCA history and audit data
- Require self-test security related GPO-PCA services
- Require a trusted path for identification of PKI roles and associated identities
- Require a recovery mechanisms for keys and the GPO-PCA system

The CSS (OCSP) system provides the following security technical controls:

- Require authenticated logins before permitting any access to the system
- Provide a security audit capability
- Enforces separations of roles and manages privileges of users to limit users to their assigned role
- Enforce domain integrity boundaries for security critical processes
- Support recovery from key or system failure

6.5.2 Computer Security Rating

There is no requirement for a computer security rating.

6.6 LIFE CYCLE TECHNICAL CONTROLS

The effectiveness and appropriateness of the security settings described in this CPS are reviewed on a yearly basis. A risk and threat assessment is performed to determine if key lengths need to be increased or operational procedures modified to maintain the required level of system security.

6.6.1 System Development Controls

The CA server hardware was purchased new and is dedicated for use as the GPO-PCA within the GPO PKI. All hardware was kept in tamper-evident sealed containers, with access restricted to authorized individuals. All access to any of the PKI hardware, prior to installation in the CA facility, was manually recorded in a paper log maintained by the OA. The OA will make this log available to the Compliance Auditors during any compliance audit.

The CA software is dedicated to providing the GPO-PCA functions. The GPO-PCA uses Entrust COTS CA software. Only OA-approved software has been loaded on the CA servers.

The CA hardware has been installed in the CA facility in accordance with the physical security safeguards as defined in this CPS. These physical safeguards serve to restrict access to the CA hardware to a limited number of trusted individuals. These physical safeguards in combination with the network security controls defined in this CPS restrict the ability for malicious software to be installed on the CA hardware.

RA hardware and software shall be scanned for malicious code on first use and periodically afterward.

6.6.2 Security Management Controls

The installation and configuration of the CA hardware and software is performed under very strict, scripted guidelines as part of the key generation ceremony with each step being videotaped and audited by the Compliance Auditor identified in this CPS.

The GPO follows a formal software implementation methodology whereby all PKI software upgrades and/or modifications to production systems are first installed and evaluated in a test

environment. All software modifications and/or upgrades are installed in a test environment and evaluated by the OA.

At the completion of the evaluation period, the GPO OA submits to the GPO PA a digitally signed production software or hardware modification request indicating the specific hardware device, software title and version number to be modified. In addition, the report indicates the new hardware device, software title and version number, as well as a list of modifications or enhancements that the new hardware or software provides. The GPO PA is responsible for reviewing and approving the production software or hardware modification request. If the GPO PA approves the request, it will be returned to the GPO OA digitally signed by the GPO PA.

6.6.3 Life Cycle Security Controls

There is no requirement for life cycle security ratings.

6.7 NETWORK SECURITY CONTROLS

Remote access to the GPO-PCA server via the RA interface is secured using the security features of the PKIX-CMP protocol. No other remote access is permitted and features including inbound FTP are disabled.

All unused network ports and services on the CA system are disabled. Network software present and operational on the CA system shall be necessary for the proper functioning of the CA system.

The network connection to the GPO-PCA server is protected by a firewall. The firewall policy is as follows.

With respect to GPO-PCA application server:

- With the exception of sessions initiated using the PKIX-CMP and TLS protocols disallow all other inbound initiated sessions to the production CA server
- With the exception of sessions initiated using the LDAP protocol to the LDAP Master Directory server, sessions initiated using the Microsoft approved protocol for Windows operating system patch updates and sessions initiated using the Symantec approved protocol for Symantec Anti-virus system updates, disallow all other outbound initiated sessions from the production CA servers

With respect to the GPO-PCA Master Directory server:

- With the exception of sessions initiated using the LDAP protocol from the GPO-PCA server, disallow all other inbound initiated sessions to the LDAP Master Directory server
- With the exception of sessions initiated using directory update protocols to the production LDAP Slave Directory servers, disallow all other outbound initiated sessions from the LDAP Master Directory server

6.8 TIME-STAMPING

Asserted times are accurate via use of the NIST clock source and the Network Time Protocol (NTP) service. Connections to the NIST clock is monitored by the GPO OA via automated

methods based on the e-Health monitoring software to ensure that times are accurate to the federal PKI Common Policy requirements. Clock adjustments are an auditable event per section 5.4.1 of this CPS and are logged in the OS logs of the GPO PCA.

7. CERTIFICATE, CRL AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

The GPO-PCA issues X.509 Version 3 certificates and supports the following fields:

- Version: Version field is set to v3
- Signature: Identifier for the algorithm used by the GPO-PCA to sign the certificate; Algorithm identifier (RSA with SHA-1 (for certificates that expire on or before December 31, 2010) or RSA with SHA-256 (for certificates that expire on or after January 1, 2011)
- Issuer: Certificate issuer (CA) Distinguished Name
- Validity: Certificate validity period - notBefore start date and notAfter end date are specified
- Subject: Certificate subject Distinguished Name
- Subject public key information:

For the actual format of certificates issued by the GPO-PCA, see Appendix A.

Certificates issued by the GPO-PCA shall be compliant with the CCP-PROF profile..

7.1.1 Version Numbers

Certificates issued by this CA are issued with the version number set to v3.

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 CPS shall use the following OIDs for signatures:

sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha-256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

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

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

For certificates issued that contain the id-fpki-common-policy, id-fpki-common-hardware, or the id-fpki-common-devices OID, the subject and issuer fields of the base certificate shall be populated with an X.500/X.501 compliant Distinguished Name, with the attribute type as further constrained by RFC2459. Certificates issued under id-fpki-common-authentication, the distinguished name shall be populated using the rules for id-fpki-common-hardware and shall conform to X.500/X.501. Certificates issued under id-fpki-common-authentication shall include a subject alternative name field, as specified in the Certificate Profile for the PIV Authentication Certificate defined in Appendix A.1.5 of this CPS.

7.1.5 Name Constraints

Name constrains are issued in CA and Cross Certificates. The GPO-PCA does not issue CA or Cross Certificates.

7.1.6 Certificate Policy Object Identifier

Certificates issued by the GPO-PCA shall assert one of the certificate policy OIDs specified in section 1.2 of this CPS. The GPO-PCA and its administrators (RA's) use the procedures in the Initial Registration section of this CPS (section 3.1) and the Certificate Registration Form to determine which OID is appropriate for the certificate being issued. For example, a certificate that will not be issued on a hardware token, cannot have the OID for id-fpki-common-hardware.

7.1.7 Usage of Policy Constraints Extension

The GPO-PCA may assert a policy constraint extension in its CA certificate.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued under this CPS shall not contain policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Certificates issued under this CPS shall not contain a critical certificate policy extension.

7.2 CRL PROFILE

For the profile of CRL and ARL issued by the GPO-PCA, see Appendix A.2.

7.2.1 Version Numbers

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

7.2.2 CRL Entry Extensions

Detailed CRL profiles addressing the use of each extension shall conform to the CCP-PROF profile.

7.3 OCSP PROFILE

For the profile of OCSP Certificates issued by the GPO-PCA, see Appendix A.7.

The CSS shall be able to process SHA-1 and SHA-256 hash values if they are included in the CertID field and the KeyHash in the responder ID field, and the CSS for the GPO-PCA is configured for this.

7.3.1 Version Numbers

The GPO-PCA shall issue Version 1 OCSP certificates, that comply with federal PKI Common Policy Framework and GPO CP requirements.

7.3.2 OCSP Entry Extensions

There shall be no critical OCSP extensions in the OCSP Profile issued by the GPO-PCA. Detailed OCSP profiles addressing the use of each extension shall conform to the CCP-PROF profile.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

Internal compliance audits shall be performed according to the federal PKI Common Policy and GPO CP requirements. Assessments shall take place upon on the initial activation of a new CA (a brand new CA or new DN for a CA) and once every 12 months thereafter for the CA and RA's in accordance with federal PKI Common Policy and GPO CP requirements. In accordance with the CP for the Federal PKI Common Policy Framework, as an alternative to a full annual compliance audit against the entire CPS, the compliance audit of the GPO-SCA and RA's may be carried out in accordance with the requirements as specified in the Triennial Audit Guidance document located at: http://www.idmanagement.gov/fpkipa.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

The GPO PA will have the responsibility to verify that the assessor or compliance auditor selected, by the GPO-OA, to audit the GPO PCA and any applicable personnel meet the requirements governing the identity and qualifications of the assessor/compliance auditor that are stipulated in the US federal PKI Common Policy and the GPO CP .The assessor or compliance auditor must perform PKI compliance audits as a regular ongoing business activity. The auditor must be a certified information system auditor (CISA) or IT security specialist (such as a certified information systems security professional or CISSP), and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The compliance auditor or assessor is a firm in a contractual relationship with the GPO and has no GPO PKI management capabilities or responsibilities.

8.4 TOPICS COVERED BY ASSESSMENT

The compliance audit verifies that the operational and technical controls used by the GPO PCA operations personnel, including all RA's, satisfy all requirements of the federal PKI Common Policy Framework, the GPO CP, and the stipulations in this CPS, including all the following topics:

- Identification & Authentication (Section 3)
  Initial Registration
  Certificate Renewal, Update, and Routine Re-key
  Re-key After Revocation
  Revocation Request
- Certificate Life-Cycle Operational Requirements (Section 4)
  Application for a Certificate
  Certificate Issuance
  Certificate Acceptance

Certificate Suspension and Revocation
Security Audit Procedures
Records Archival
Key Changeover
Compromise and Disaster Recovery
CA Termination

- Facility, Management, and Operational Controls (Section 5)

  Physical Controls
  Procedural Controls
  Personnel Controls
- Technical Security Controls (Section 6)

  Key Pair Generation & Installation
  Private Key Protection
  Other Aspects of Key Pair Management
  Activation Data
  Computer Security Controls
  Life-cycle Technical Controls
  Network Security Controls
  Cryptographic Module Engineering Controls
- Certificate, CRL and OCSP Profiles (Section 7)

  Certificate Profile
  ARL/CRL Profile
- Specification Administration (Section 8)

  Specification Change Procedures
  Publication and Notification Procedures
  CPS Approval Procedures

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

There are three possible actions to take when a deficiency has been identified:

- Continue to operate as usual
- Continue to operate but at a lower assurance level
- Suspend operation

If a deficiency is identified, the GPO PA will determine which of the following actions to take.

- If continuing operation, as usual or lower assurance level, the GPO PA and OA are responsible for ensuring that corrective actions are taken within 30 days. At that time, or earlier if agreed by the GPO PA and Compliance Auditor, the compliance audit team will re-audit the GPO PCA in the areas of deficiencies. If, upon re-audit, corrective actions have not been taken, the GPO PA will determine if more severe action is required.
- If operation is suspended the GPO PA and OA are responsible for reporting the status of corrective action to the Compliance Auditors on a weekly basis. The GPO PA and Compliance Auditor together will determine when re-audit is to occur. If the deficiencies are deemed to have been corrected upon re-audit, the GPO PCA will resume service.

8.6 COMMUNICATIONS OF RESULTS

The compliance auditor will communicate results of all compliance audits to the PA through a Compliance Audit Report. The report will contain a summary table of topics covered, areas in which the GPO PCA was found to be non-compliant and a brief description of the problems for each area of non-compliance. The report will also contain the detailed results of the compliance audit for all topics covered, including the topics in which the GPO PCA passed and the topics in which the GPO PCA failed. The GPO PCA Operational Authority (OA) shall propose remedies for any topic failure, including expected time for completion, to the federal PKI Policy Authority and the GPO PA.

Notification of compliance audit failure, the topics of failure and, reasons for failure will be provided immediately, upon the conclusion of the compliance audit, in a written report to the GPO PCA OA, the GPO PA, and the federal PKI Policy Authority.

The audit compliance report shall be provided to the GPO PA and OA, and to the federal PKI Policy Authority. The audit report and identification of corrective measures to the federal PKI Policy Authority and the GPO PA within 30 days of completion. A special compliance audit shall be conducted if it is required to confirm the implementation and effectiveness of the remedy. The federal PKI Policy Authority can determine that such a special compliance audit is required to verify implementation and effectiveness of the remedy, and the GPO PA can do so as well.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 Certificate Issuance or Renewal Fees

GPO fees for certificate issuance and renewal are set by GPO and documented with Subscribers.

9.1.2 Certificate Access Fees

There are no charges for access to the GPO-PCA certificate or to Subscriber certificates.

9.1.3 Revocation or Status Information Access Fees

There are no charges for access to Revocation, CRL or CSS Status information.

9.1.4 Fees for Other Services

GPO reserves the right to set fees in accordance with this CPS and MOA's for other services provided by the GPO-PCA.

9.1.5 Refund Policy

Refunds are subject to a case by case review by GPO and the Subscriber's organization.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

There is no insurance coverage for any non-GPO or external party.

9.2.2 Other Assets

No stipulations.

9.2.3 Insurance or Warranty Coverage for End-Entities

There is no insurance coverage or warranty coverage of any kind for end-entities or for relying parties offered by the GPO-PCA.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

GPO-PCA information not requiring protection may be made publicly available, according to the stipulations of this CPS in the sub-sections below.

9.3.1 Scope of Confidential Information

Each Subscriber's private signing key is confidential to that Subscriber. The CA and RA are not provided any access to those keys.

Information held in audit logs and the archives is considered confidential to the GPO-PCA and is not released to external parties, unless required by law.

Personal information held by the RA, other than that which is explicitly published as part of a certificate, CRL, CP or this CPS is considered confidential to the GPO PKI and is not released unless required by law.

Information in transit between the RA and the GPO-PCA is automatically encrypted by the GPO-PCA and RA components to provide data confidentiality. Information stored on the RA workstation or GPO-PCA server is protected by password. The RA keeps paper information (e.g., registration forms) in a locked container when the RA is not present.

9.3.2 Information Not Within Scope of Confidential Information

Information included in certificates and CRLs issued by the GPO-PCA are not considered confidential, with the exception of the FASC-N value in the subject alternative name extension in all common-authentication (PIV Authentication) and GPO Authentication certificates.

.

9.3.3 Responsibility to Protect Confidential Information

The GPO-PCA PA and OA shall have responsibility to ensure that controls exist to protect the confidential information in section 9.3.1.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

A Privacy Impact Assessment (PIA) for the GPO-PCA shall be produced by GPO and shall involve the GPO Privacy Officer. The PIA shall be made available to the compliance auditor and the Federal PKI Policy Authority.

9.4.2 Information Treated as Private

Information held in the GPO-PCA audit logs and the GPO-PCA archives is considered private and shall not released to external parties (with the exception of the Federal PKI Policy Authority), unless required by law.

9.4.3 Information not Deemed Private

Information included in certificates and CRLs issued by the GPO-PCA are not considered confidential, with the exception of the FASC-N value in the subject alternative name extension in all common-authentication (PIV Authentication) and GPO Authentication certificates.

9.4.4 Responsibility to Protect Private Information

The GPO-PCA PA and OA shall have responsibility to ensure that controls are in force and operational to securely store and protect the private information discussed in section 9.4.

9.4.5 Notice and Consent to Use Private Information

There are no requirements for the GPO-PCA to provide notice or obtain consent to use the information provided by Subscribers and applicants for certificates.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The GPO PA is the responsible party to review all requests for information release as part of civil discovery and, working with the GPO Policy Authority, GPO General Counsel and federal PKI Policy Authority, shall ensure that no private information or GPO-PCA information is disclosed unless required by applicable law or ordered by a court with valid jurisdiction.

The GPO PA keeps copies, either paper or electronic, of each request for information release pursuant to judicial or administrative process, and to law enforcement officials.

9.4.7 Other Information Disclosure Circumstances

None.

9.5 INTELLECTUAL PROPERTY RIGHTS

The GPO PA and OA shall comply with intellectual property rights.

All Certificates and CRLs issued by the GPO-PCA are the property of the GPO-PCA. This CPS is the property of the GPO-PCA. The Distinguished Names (DNs) for GPO entities within the GPO-PCA domain in the directory and in certificates issued to GPO entities within that domain are the property of GPO. The DNs for non-GPO entities are subject to the MOA between the entity and GPO.

With respect to licensed applications, this CPS does not modify ownership of licensed applications or licensing agreements for such applications.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CA Representations and Warranties

The GPO-PCA who issues certificates that assert this policy shall comply with the stipulations of the US federal PKI Common Policy and will comply with the requirements set forth in any MOA's that may be appropriately executed. The GPO-PCA shall make GPO certificates and CRL's available in a repository for subscribers, PKI administrators and Relying Parties use.

The GPO-PCA does not disclaim any responsibilities required under the federal PKI Common Policy Framework.

The GPO-PCA may use a variety of mechanisms for posting information into a repository as required by the US federal PKI Common Policy. These mechanisms at a minimum shall include:

- All CA certificates and CRL's shall be placed into a X.500 Directory Server System that is publicly accessible through the Lightweight Directory Access Protocol (LDAP)
- All CA certificates and CRL's shall also be available and publicly accessible via the Hyper Text Transport Protocol (HTTP)
- The GPO-PCA may optionally publish subscriber certificates into the publicly accessible X.500 Directory Server System that is publicly accessible through LDAP protocol
- Availability of the information as required by the certificate information posting and retrieval stipulations of the US federal PKI Common Policy and the GPO CP

- Access control mechanisms when needed to protect repository information from unauthorized modification or deletion (as described in later sections)
- There shall be redundant directory systems (a total of 3 directory systems for triple redundancy) at the primary operational site and in addition, redundant directory systems at the off-site backup operational site (a total of 3 directory systems for triple redundancy at the off-site backup location) so that the GPO-PCA can achieve the Common Policy directory availability requirements.
- The publicly accessible directory systems and LDAP and HTTP access mechanisms shall be operated and maintained to comply with the Federal PKI Common Policy Framework requirements for overall availability, and the scheduled downtime for these systems will be limited to ensure that Federal PKI Common Policy Framework requirements are met at all times
  - The schedule downtime requirements in the federal PKI Common Policy are met by tracking all scheduled downtime in GPO PKI Change Control Records and ensuring that one of the redundant systems is always planned to be online and active, to avoid any downtime while other redundant systems might undergo scheduled maintenance or problem resolution.

9.6.1.1 Certificate Issuance to Non-GPO Parties

The GPO-PCA may issue certificates to non-GPO parties, as established by the GPO-PA and in accordance with the federal PKI Common Policy requirements. A Subscriber Agreement or similar instrument will be executed, and will contain provisions that comply with the federal PKI Common Policy requirements.. All subscribers will be registered as described below in Section 3.1, Initial Registration, including procedures as specified below for device certificates for non-human subscribers. .

9.6.1.2 Certificate Status Server Representations and Warranties

The GPO-PCA shall provide redundant Certificate Status Server (CSS) (also known as OCSP servers) to achieve the federal PKI Common Policy availability requirements. There shall be a backup OCSP server at the off-site backup location, to provide a redundant capability, in order to provide redundancy for the required CSS capability and achieve the federal PKI Common Policy availability requirements.

The CSS shall be operated and maintained to comply with the Federal PKI Common Policy Framework requirements for overall availability, and the scheduled downtime for these redundant systems will be limited to ensure that Federal PKI Common Policy Framework requirements for limiting scheduled downtime is met at all times.

The schedule downtime requirements in the federal PKI Common Policy are met by tracking all scheduled downtime for the CSS sysem in GPO PKI Change Control Records and ensuring that one of the redundant systems is always planned to be online and active, to avoid any downtime while the other redundant system might undergo scheduled maintenance or problem resolution.

9.6.2 RA Representations and Warranties

The RA will abide by all obligations and all stipulations defined in the US federal PKI Common Policy for Common-Policy, Common-Authentication, Common-Hardware, Common-cardAuth, and Common-Device certificates, for all GPO CP obligations, and shall also abide by this CPS. The RA shall ensure that the cryptographic module shall not left unattended once the private key is activated, in order to ensure that unauthorized access to the private key does not occur.

RA's shall conform to the stipulations of the federal PKI Common Policy and this CPS including:

- Maintaining RA operations in conformance with this CPS
- Including only valid and appropriate information in certificate requests, and maintaining evidence that due diligence was exercised in validating the information contained in the certificate
- Ensuring that obligations are imposed on Subscribers via the Subscriber Agreement, and that Subscribers are informed of the consequences of not complying with the obligations contained in the Subscriber Agreement and this CPS (by informing Subscribers that their certificate can be revoked for non-compliance with the Subscriber Agreement and this CPS).

RA's that are found to have acted in a manner inconsistent with these obligations in this CPS or the Federal PKI Common Policy shall be subject to revocation of RA responsibilities.

9.6.3 Subscriber Representations and Warranties

Subscriber obligations are specified in the Subscriber agreement, including requirements for protecting the private key and use of the certificate,that each Subscriber applicant must sign prior to the time they receive their keys and certificates. This agreement includes an obligation that the cryptographic module shall not be left unattended by the Subscriber once the private key is activated. These requirements apply to human sponsors associated with Device certificates issued under id-fpki-common-devices.

9.6.4 Relying Party Representations and Warranties

The US federal Common Policy 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-PCA 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-PCA shall make GPO certificates and CRL's available in

a repository and shall also make certificate status available via OCSP so that Relying Parties may obtain GPO certificates and CRL's for Relying Party use (pursuant to Relying Party policies).

The Relying Party must determine if the certificates issued under the GPO-PCA are appropriate for their application. This may 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.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 DISCLAIMERS OF WARRANTIES

The GPO-PCA does not disclaim any responsibilities required by the federal PKI Common Policy or the GPO Certificate Policy.

9.8 LIMITATIONS OF LIABILITY

The GPO shall not liable to any party with respect to the operations of the GPO-PCA except in accordance with federal law, or through a valid express written contract between GPO and another party.

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 or revoked by, or not revoked by, the GPO-PCA.

Certificates are issued and revoked at the sole discretion of the GPO-PA. When the GPO-PCA issues a cross-certificate, it does so for the convenience of the GPO and in compliance with the provisions of the US federal PKI Common Policy and the GPO CP. The Entity must determine whether the US Federal PKI Common Policy or 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 the CP by the Entity, including Relying Parties.

9.9 INDEMNITIES

No stipulation.

9.10 TERM AND TERMINATION

9.10.1 Term

This CPS becomes effective when approved by the GPO PA and OA. There is no specified term for this CPS.

9.10.2 Termination

Termination of this CPS is at the discretion of the GPO PA. The Federal PKI Policy Authority shall be notified by email and telephone if this CPS is terminated.

9.10.3 Effect of Termination and Survival

The effects of this CPS apply until the end of the archive period of the last certificate issued by the GPO-PCA.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

The GPO PA shall notify and communicate with participants via instructions and methods contained in MOA's.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

The GPO PA shall review this CPS at least annually. Corrections or changes to this CPS shall be made available to all Subscribers and Participants, via publication of the CPS on the Internet at the GPO PKI web site (http://www.gpo.gov/projects/pki.htm).

Suggested changes to this CPS may be provided to the Contact Person listed in section 1.5.2 of this CPS. Such suggested change must include a description of the change, a justification for why the change should be implemented and contact information for the requestor.

9.12.2 Notification Mechanism and Period

Changes to this CPS shall be communicated to the Federal PKI Policy Authority (FPKIPA) in accordance with the MOA between the GPO and the FPKIPA. In addition, changes to this CPS shall be communicated to all non-GPO agencies that have an MOA in effect with the GPO PA via electronic mail (email) to the contact person listed in the MOA.

9.12.3 Circumstances under which OID must be Changed

An OID will be changed if the GPO PA or FPKIPA determine that the assurance level of the certificates do not meet the applicable GPO CP or Federal PKI Common Policy.

9.13 DISPUTE RESOLUTION PROVISIONS

The GPO PA resolves any disputes over the interpretation or applicability of the CPS.

9.14 GOVERNING LAW

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

9.15 COMPLIANCE WITH APPLICABLE LAW

The GPO-PCA shall comply with applicable law.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

Should it be determined that any relevant section of the Federal PKI Common Policy or the GPO Certificate Policy is incorrect or invalid, all parties with certificates issued by the GPO-PCA will nevertheless abide by the practices as described in this CPS, until guidance is given for new policy and a new CPS is published and communicated. Section 9.12 describes the process for changing this CPS.

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

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 OTHER PROVISIONS

No stipulation.

10. BIBLIOGRAPHY

The following documents were used in developing this CPS:

- Federal Common Policy Framework
- GPO Certificate Policy
- Federal PKI Certificate Profile
- ITU X.509 Specification
- ITU X.500 Specifications

11. ACRONYMS AND ABBREVIATIONS

This section contains a list of acronyms used in this document, which is below:

ARL	Authority Revocation List
CA	Certification Authority
	Certificate Authority
CP	Certificate Policy
CPS	Certification Practices Statement
CPWG	Certificate Policy Working Group
CARL	Certification Authority Revocation List
CRL	Certificate Revocation List
CSS	Certificate Status Server
FBCA	Federal Bridge Certification Authority
FPKI	Federal PKI
FPKI PA	Federal PKI Policy Authority
GPO	Government Printing Office
HSM	Hardware Security Module
LDAP	Lightweight Directory Access Protocol
OA	Operational Authority
OCSP	Online Certificate Status Protocol
PA	Policy Authority
PCA	Principal Certification Authority
PKI	Public Key Infrastructure
RA	Registration Authority
SCA	Subordinate Certification Authority

SABO	System Administrator and Backup Operator

12. 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 Entitiy 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]

13. ACKNOWLEDGEMENTS

The GPO OA and authorized contractor support personnel developed this CPS.

APPENDIX A: Certificate, CRL and OCSP Profiles

This appendix contains the profiles for the certificates, CRL's and OCSP responses issued by the GPO-PCA.

A.1 PCA (ROOT CA) SELF-SIGNED CERTIFICATE FORMAT

Field	GPO Root CA Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-256WithRSAEncrytion {1 2 840 113549 1 1 11}
Issuer Distinguished Name	ou=GPO PCA, ou=Certification Authorities, ou=Government Printing Office, o=U.S. Government, c=US
Validity Period	20 years from date of issue in Generalized Time format
Subject Distinguished Name	ou=GPO Root CA, ou=Certification Authorities, ou=Government Printing Office, o=U.S. Government, c=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha-256WithRSAEncrytion {1 2 840 113549 1 1 11}
Extensions	
Authority key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the GPO Root CA's public key information)
subject key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the GPO Root CA's public key information)
key usage	c=no; digitalSignature, keyCertSign, cRLSign
Basic Constraints	c=no; cA=True; no path length constraint

A.2 SUBORDINATE CA (SCA) CERTIFICATE FORMAT

Field	Subordinate CA Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-256WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	ou=GPO Root CA, ou=Certification Authorities, ou=Government Printing Office, o=U.S. Government, c=US
Validity Period	Depends on the Assurance level of the CA
Subject Distinguished Name	ou=<CA Name>, ou=Certification Authorities, ou=Government Printing Office, o=U.S. Government, c=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha-256WithRSAEncryption {1 2 840 113549 1 1 5}
Extensions	
Authority key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the GPO Root CA's public key information)
subject key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the Subject CA's public key information)
key usage	c=yes; digitalSignature, keyCertSign, cRLSign
Certificate policies	c=no; {2 16 840 1 101 3 2 1 17 1}
Basic Constraints	c=yes; cA=True; path length constraint = 0
Policy Constraints	Not Present
Authority Information Access	C=no; optional; pointer to OCSP Responder
CRL Distribution Points[1]	c = no; always present

1 The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

A.3 EXTERNAL CA CERTIFICATE FORMAT

Field	Subordinate CA Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-256WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	ou=GPO PCA, ou=Certification Authorities, ou=Government Printing Office, o=U.S. Government, c=US
Validity Period	Depends on the assurance level of the CA
Subject Distinguished Name	As designated by the GPO PA
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha-256WithRSAEncryption {1 2 840 113549 1 1 5}
Extensions	
Authority key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the GPO Root CA's public key information)
subject key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the Subject CA's public key information)
key usage	c=yes; digitalSignature, keyCertSign, cRLSign
Certificate policies	c=no; {2 16 840 1 101 3 2 1 15 i} i = 1, 2, 3, and/or 4[1]
Policy Mapping	Maps each of the policies listed in the Certificate Policies extension listed above to subject CA domain policy
Basic Constraints	c=yes; cA=True; path length constraint absent
Name Constraints	c=yes; permitted subtrees: <TBD>; excluded subtrees: ou=Government Printing Office, o=U.S. Government, c=US
Policy Constraints	c=yes; inhibit policy mapping skipCerts = 0, 1, 2[2]; require explicit policy, skipCerts = 0/
Authority Information Access	C=no; optional; pointer to OCSP Responder
CRL Distribution Points[3]	c = no; always present

1 The field shall contain all certificate policies that are equal to or lower. For example, for a medium assurance CA, there will be three OIDs in the field.

2 Value of 0 for cross certificate to other domain, value of 1 for a Bridge CA, value of 2 for a Bridge CA with membrane and commitment to have proper skipCerts value.

3 The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

A.4 ROOT CA CRL PROFILE FORMAT

Field	Root CA CRL Value
Version	V2 (1)
Issuer Signature Algorithm	sha-256WithRSAEncrytion {1 2 840 113549 1 1 11}
Issuer Distinguished Name	ou=GPO PCA, ou=Certification Authorities, ou=Government Printing Office, o=U.S. Government, c=US
thisUpdate	UTCT
nextUpdate	UTCT; thisUpdate + 28 days
Revoked certificates list	0 or more 2-tuple of certificate serial number and revocation date (in UTCT)
CRL extensions	
CRL Number	Integer
Authority Key Identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the GPO Root CA's public key information)
CRL entry extensions	
Invalidity Date	Optional
Reason Code	Always Present; Will not include certificateHold

A.5 FEDERAL COMMON POLICY CERTIFICATE FORMAT

Field	Principal CA Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-256WithRSAEncrytion {1 2 840 113549 1 1 11}
Issuer Distinguished Name	
Validity Period	
Subject Distinguished Name	ou= GPO PCA, ou=Certification Authorities, ou=Government Printing Office, o=U.S. Government, c=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}

Field	Principal CA Value
Extensions	
Authority key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the GPO Root CA's public key information)
subject key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the Subject CA's public key information)
key usage	c=yes; digitalSignature, keyCertSign, cRLSign
Certificate policies	c=no; {2 16 840 1 101 3 2 1 3 6}
Basic Constraints	
CRL Distribution Points	
Authority Information Access	
Subject Information Access	

A.5.1 FEDERAL COMMON-HARDWARE CERTIFICATE FORMAT

Field	Principal CA Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-256WithRSAEncrytion {1 2 840 113549 1 1 11}
Issuer Distinguished Name	
Validity Period	
Subject Distinguished Name	ou= GPO PCA, ou=Certification Authorities, ou=Government Printing Office, o=U.S. Government, c=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Extensions	
Authority key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the GPO Root CA's public key information)
subject key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the Subject CA's public key information)
key usage	c=yes; digitalSignature, keyCertSign, cRLSign
Certificate policies	c=no; {2 16 840 1 101 3 2 1 3 7}

Field	Principal CA Value
Basic Constraints	
CRL Distribution Points	
Authority Information Access	
Subject Information Access	

A.5.2 COMMON POLICY SIGNATURE CERTIFICATE PROFILE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} (for certificates that expire on or before December 31, 2010); or sha-256WithRSAEncrytion {1 2 840 113549 1 1 11} (for certificates that expire on or after January 1, 2011)
Algorithm Identifier	
Issuer Distinguished Name	ou= GPO PCA, ou=Certification Authorities, ou=Government Printing Office, o=U.S. Government, c=US
Validity Period	
Subject Distinguished Name	
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Extensions	
Authority key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the GPO Root CA's public key information)
Subject key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the Subject CA's public key information)
key usage	c=yes; digitalSignature, nonRepudiation
Certificate policies	
CRL Distribution Points	
Authority Information Access	
Issuer Alt Name	
Subject Alt Name	

A.5.3 COMMON POLICY KEY MANAGEMENT CERTIFICATE PROFILE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} (for certificates that expire on or before December 31, 2010); or sha-256WithRSAEncrytion {1 2 840 113549 1 1 11} (for certificates that expire on or after January 1, 2011)
Issuer Distinguished Name	ou= GPO PCA, ou=Certification Authorities, ou=Government Printing Office, o=U.S. Government, c=US
Validity Period	
Subject Distinguished Name	
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Extensions	
Authority key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the GPO Root CA's public key information)
Subject key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the Subject CA's public key information)
key usage	c=yes; keyEncipherment
Certificate policies	
CRL Distribution Points	
Authority Information Access	
Issuer Alt Name	
Subject Alt Name	

A.5.4 COMMON POLICY DEVICE CERTIFICATE PROFILE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} (for certificates that expire on or before December 31, 2010); or sha-256WithRSAEncrytion {1 2 840 113549 1 1 11} (for certificates that expire on or after January 1, 2011)
Issuer Distinguished Name	ou= GPO PCA, ou=Certification Authorities, ou=Government Printing Office, o=U.S. Government, c=US
Validity Period	
Subject Distinguished Name	
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Extensions	
Authority key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the GPO Root CA's public key information)
Subject key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the Subject CA's public key information)
key usage	c=yes; digitalSignature, keyEncipherment
Certificate policies	id-fpki-common-devices {2.16.840.1.101.3.2.1.3.8}
CRL Distribution Points	
Authority Information Access	
Issuer Alt Name	
Subject Alt Name	

A.5.5 COMMON POLICY CARD AUTHENTICATION CERTIFICATE PROFILE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} (for certificates that expire on or before December 31, 2010); or sha-256WithRSAEncrytion {1 2 840 113549 1 1 11} (for certificates that expire on or after January 1, 2011)
Issuer Distinguished Name	ou= GPO PCA, ou=Certification Authorities, ou=Government Printing Office, o=U.S. Government, c=US
Validity Period	
Subject Distinguished Name	
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Extensions	
Authority key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the GPO Root CA's public key information)
Subject key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the Subject CA's public key information)
key usage	c=yes; digitalSignature
Extended key usage	Yes; id-PIV-cardAuth {2.16.840.1.101.3.6.8}
Certificate policies	id-fpki-common-cardAuth {2.16.840.1.101.3.2.1.3.17}
CRL Distribution Points	
Authority Information Access	
Issuer Alt Name	
Subject Alt Name	Piv-interim (Boolean); {2.16.840.1.101.3.6.9.1}

A.5.6 COMMON POLICY PIV AUTHENTICATION CERTIFICATE PROFILE

(NOTE: Certificates with this Profile shall not be distributed in public repositories (e.g., via LDAP or HTTP.)

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} (for certificates that expire on or before December 31, 2010); or sha-256WithRSAEncrytion {1 2 840 113549 1 1 11} (for certificates that expire on or after January 1, 2011)
Issuer Distinguished Name	ou= GPO PCA, ou=Certification Authorities, ou=Government Printing Office, o=U.S. Government, c=US
Validity Period	
Subject Distinguished Name	
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Extensions	
Authority key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the GPO Root CA's public key information)
Subject key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the Subject CA's public key information)
key usage	c=yes; digitalSignature
Certificate policies	id-fpki-common-authentication {2.16.840.1.101.3.2.1.3.13}
CRL Distribution Points	
Authority Information Access	
Issuer Alt Name	

Field	Value
Subject Alt Name	otherName {FASC-N value} type-id {2.16.840.1.101.3.6.6} otherName {UPN OtherName OID} type-id {1.3.6.1.4.1.311.20.2.3} value=UTF8String
piv-interim	{2.16.840.1.101.3.6.9.1} Interim_indicator (Boolean)

A.6.1 GPO MEDIUM ASSURANCE POLICY CERTIFICATE FORMAT

Field	Principal CA Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-256WithRSAEncrytion {1 2 840 113549 1 1 11}
Issuer Distinguished Name	
Validity Period	
Subject Distinguished Name	ou= GPO PCA, ou=Certification Authorities, ou=Government Printing Office, o=U.S. Government, c=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Extensions	
Authority key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the GPO Root CA's public key information)
subject key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the Subject CA's public key information)
key usage	c=yes; digitalSignature, keyCertSign, cRLSign
Certificate policies	c=no; {2 16 840 1 101 3 2 1 17 1}
Basic Constraints	
CRL Distribution Points	
Authority Information Access	
Subject Information Access	

A.6.2 GPO MEDIUM-HARDWARE POLICY CERTIFICATE FORMAT

Field	Principal CA Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-256WithRSAEncrytion {1 2 840 113549 1 1 11}
Issuer Distinguished Name	
Validity Period	
Subject Distinguished Name	ou= GPO PCA, ou=Certification Authorities, ou=Government Printing Office, o=U.S. Government, c=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Extensions	
Authority key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the GPO Root CA's public key information)
subject key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the Subject CA's public key information)
key usage	c=yes; digitalSignature, keyCertSign, cRLSign
Certificate policies	c=no; {2 16 840 1 101 3 2 1 17 2}
Basic Constraints	
CRL Distribution Points	
Authority Information Access	
Subject Information Access	

A.6.3 GPO POLICY END ENTITY SIGNATURE CERTIFICATE PROFILE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} (for certificates that expire on or before December 31, 2010); or sha-256WithRSAEncrytion {1 2 840 113549 1 1 11} (for certificates that expire on or after January 1, 2011)
Algorithm Identifier	
Issuer Distinguished Name	ou= GPO PCA, ou=Certification Authorities, ou=Government Printing Office, o=U.S. Government, c=US
Validity Period	
Subject Distinguished Name	
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Extensions	
Authority key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the GPO Root CA's public key information)
Subject key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the Subject CA's public key information)
key usage	c=yes; digitalSignature, nonRepudiation
Certificate policies	
CRL Distribution Points	
Authority Information Access	
Issuer Alt Name	
Subject Alt Name	

A.6.4 GPO POLICY KEY MANAGEMENT CERTIFICATE PROFILE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} (for certificates that expire on or before December 31, 2010); or sha-256WithRSAEncrytion {1 2 840 113549 1 1 11} (for certificates that expire on or after January 1, 2011)
Issuer Distinguished Name	ou= GPO PCA, ou=Certification Authorities, ou=Government Printing Office, o=U.S. Government, c=US
Validity Period	
Subject Distinguished Name	
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Extensions	
Authority key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the GPO Root CA's public key information)
Subject key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the Subject CA's public key information)
key usage	c=yes; keyEncipherment
Certificate policies	
CRL Distribution Points	
Authority Information Access	
Issuer Alt Name	
Subject Alt Name	

A.6.5 GPO POLICY MEDIUM DEVICE CERTIFICATE PROFILE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} (for certificates that expire on or before December 31, 2010); or sha-256WithRSAEncrytion {1 2 840 113549 1 1 11} (for certificates that expire on or after January 1, 2011)
Issuer Distinguished Name	ou= GPO PCA, ou=Certification Authorities, ou=Government Printing Office, o=U.S. Government, c=US
Validity Period	
Subject Distinguished Name	
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Extensions	
Authority key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the GPO Root CA's public key information)
Subject key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the Subject CA's public key information)
key usage	c=yes; digitalSignature, keyEncipherment
Certificate policies	id-gpo-certpcy-devices {2 16 840 1 101 3 2 1 17 3}
CRL Distribution Points	
Authority Information Access	
Issuer Alt Name	
Subject Alt Name	

A.6.6 GPO POLICY CARD AUTHENTICATION CERTIFICATE PROFILE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} (for certificates that expire on or before December 31, 2010); or sha-256WithRSAEncrytion {1 2 840 113549 1 1 11} (for certificates that expire on or after January 1, 2011)
Issuer Distinguished Name	ou= GPO PCA, ou=Certification Authorities, ou=Government Printing Office, o=U.S. Government, c=US
Validity Period	
Subject Distinguished Name	
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Extensions	
Authority key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the GPO Root CA's public key information)
Subject key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the Subject CA's public key information)
key usage	c=yes; digitalSignature
Extended key usage	Yes; id-GPO-cardAuth {2.16.840.1.101.3.2.1.17}
Certificate policies	id-gpo-certpcy-cardAuth {2 16 840 1 101 3 2 1 17 5}
CRL Distribution Points	
Authority Information Access	
Issuer Alt Name	
Subject Alt Name	GPO-interim (Boolean); {2.16.840.1.101.3.2.1.17}

A.6.7 GPO POLICY AUTHENTICATION CERTIFICATE PROFILE

(NOTE: Certificates with this Profile shall not be distributed in public repositories (e.g., via LDAP or HTTP.)

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} (for certificates that expire on or before December 31, 2010); or sha-256WithRSAEncrytion {1 2 840 113549 1 1 11} (for certificates that expire on or after January 1, 2011)
Issuer Distinguished Name	ou= GPO PCA, ou=Certification Authorities, ou=Government Printing Office, o=U.S. Government, c=US
Validity Period	
Subject Distinguished Name	
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Extensions	
Authority key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the GPO Root CA's public key information)
Subject key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the Subject CA's public key information)
key usage	c=yes; digitalSignature
Certificate policies	id-gpo-certpcy-authentication {2 16 840 1 101 3 2 1 17 4}
CRL Distribution Points	
Authority Information Access	
Issuer Alt Name	

Field	Value
Subject Alt Name	otherName {FASC-N value} type-id {2.16.840.1.101.3.6.6} otherName {UPN OtherName OID} type-id {1.3.6.1.4.1.311.20.2.3} value=UTF8String
piv-interim	{2.16.840.1.101.3.6.9.1} Interim_indicator (Boolean)

A.7 GPO-PCA OCSP PROFILE FORMAT

Field	Value
Version	V1 (0)
Serial Number	Must be unique
Signature Algorithm	sha-256WithRSAEncrytion {1 2 840 113549 1 1 11} (for certificates that expire on or after January 1, 2011)
Issuer Distinguished Name	ou= GPO PCA, ou=Certification Authorities, ou=Government Printing Office, o=U.S. Government, c=US
Validity Period	
Subject Distinguished Name	
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Extensions	
Authority key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the GPO Root CA's public key information)
Subject key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the Subject CA's public key information)
key usage	c=yes; digitalSignature
Extended key usage	Yes; id-kp-OCSPSigning {1.3.6.1.5.5.7.3.9}
Certificate policies	id-gpo-certpcy-devices {2.16.840.1.101.3.2.1.17.3}
CRL Distribution Points	
Authority Information Access	
Issuer Alt Name	
Subject Alt Name	Piv-interim (Boolean); {2.16.840.1.101.3.6.9.1}

A.8 GPO-PCA CERTIFICATE REGISTRATION DATA REQUIREMENTS

The GPO PKI Certificate Registration Form (depicted below) defines the data required to be submitted by subscribers to the GPO-PCA for certificate issuance.

GPO PKI Certificate Registration Form

GPO PKI Registration Form **SECTION 1 (This section to be completed by applicant prior to in-person Registration)**

USER INFORMATION (Please print)					
First Name		Middle Name		Last Name	
Email Address				Telephone#	
User's Agency Name (print):					
User's Address:					
Fed. Gov't-issued Picture ID	ID#		Type		
Fed. Gov't-issued Picture ID	ID#		Type		
Non-Fed. Gov't-issued Picture ID	ID#		Type		
Non-Fed. Gov't-issued Picture ID or ID	ID#		Type		
Supervisor Signature: I declare under penalty of perjury that the foregoing is true and correct. Executed on: _____(date) Signature: _____					
Supervisor Name (Printed):					
User Signature: I declare under penalty of perjury that the foregoing is true and correct. Executed on: _____(date) Signature: _____					

SECTION 2. (This section to be completed by Registration Authority and User at time of Registration)

RA INFORMATION (Please print)			
RA First Name		RA Last Name	
RA Telephone #		RA Email Address	
Date of Registration Request	Date:		
Fed. Gov't-issued Picture ID verified	☐ Yes ☐ No ☐ N/A		
Non-Fed. Gov't-issued Picture ID verified	☐ Yes ☐ No ☐ N/A		
Non-Fed. Gov't-issued ID verified	☐ Yes ☐ No ☐ N/A		

PKI Credential Type (software or smartcard)	☐ Software (.epf file) ☐ Smartcard
Smartcard Type (if smartcard credential): (vendor and model number)	Smartcard Serial Number: (if smartcard credential)
PKI Credential Issuance Completed ☐ Yes ☐ No	Date and Time:
User Name (CN)	cn = _____
User Name (print)	User's Agency Name (print):
User Signature I declare under penalty of perjury that the foregoing is true and correct. Executed on: _____(date) Signature: _____	
RA Signature I declare under penalty of perjury that the foregoing is true and correct. Executed on: _____(date) Signature: _____	