

UNCLASSIFIED



**UNITED STATES**

**The Department of the Treasury**

**Public Key Infrastructure (PKI)**

**X.509 Certificate Policy**

Version 3.6

December 15, 2022

---

PKI Policy Management Authority (PMA)  
Daniel W. Wood

---

DATE

## Revision History

Version	Date	Author(s)	Description	Reason For Change
2.0	January 2008	James Schminky	Department of the Treasury PKI Policy in RFC 3647 format.	Bring the Treasury PKI Policy into compliance with FPKIPA change proposal requiring all cross certified PKI Policies to be in RFC 3647 format.
2.1	March 17, 2009	James Schminky	Errata changes to sections 2.2.1, 4.8, 4.9.12, 5.5, and 7.1.3.	As a result of mapping the Treasury PKI Policy to Federal Policy, a number of minor changes and omissions were identified and corrected.
2.2	March 11, 2010	James Schminky	Errata changes to sections 5.6, and 6.3.2. Change proposal changes to 2.4, 4.2.2, 5.1, 5.1.1, 5.1.2.1, 5.4.4, 5.4.5, 6.1.6, 6.5.1, and 6.7.	As a result of the PMA annual review a number of minor corrections, Federal Bridge Certification Authority (FBCA) Policy Change Proposal Number: 2009-02 and 2010-01, and Treasury Change Proposal
2.3	April 15, 2010	James Schminky	Change proposal changes to 8.1 and 8.4.	As a result of FBCA Policy Change Proposal Number: 2010-02.
2.4	March 22, 2011	James Schminky	Changes Proposal Changes to 1.3.1.8, 3.1.1&2, 3.1.5, 3.2.3.1, 4.7, 6.1.5, 8.1, and 9.4.3.	As a result of FBCA Policy Change Proposal Numbers; 2010-3 thru 8 and CPCA policy Change Proposal Number: 2011-1
2.5	September 11, 2012	Daniel Wood	Changes Proposal Changes to 3.2.3.2 and 4.9.7	Made changes to align the Treasury CP with the Common Policy Framework (CPF), removed all reference to the acronym "DoT" and replaced with the name "Treasury".
2.6	October 15, 2012	Daniel Wood	Changes Proposal Changes to 1.2, 3.2.3.2, 6.1.5, 6.2.3, 6.2.4.2, and 6.2.8.	Made changes to align the Treasury CP with the CPF,
2.7	August 22, 2013	Fred Asomani-Atinkah	1.3, 1.3.1, 1.3.1.1, 1.3.1.2, 1.3.1.3, 1.3.1.4, 1.3.1.5, 1.5.2, and 3.2.3.2.	Made changes to align the Treasury CP with the CPF,
2.8	March 26, 2015	Daniel Wood, Terry McBride	Clarified Treasury's dual role as Federal Legacy and SSP; Added PIV-I, role-based, and group certificates	Provide capabilities to customers and baseline update as requested by FPKIPA

**UNCLASSIFIED**

Version	Date	Author(s)	Description	Reason For Change
2.9	March 25, 2017	Daniel Wood	Adds PIV-I, and Internal PKI OIDs, changed criteria for suspension, defined the PKI Program Team, added the internal PKI addendum, changes to Common/Federal CPs and editorial updates	Changes to Treasury PKI based on user needs
2.91	November 20, 2018	Daniel Wood	Update based on TOCA Compliance Audit and introduction of the Fed Key Recovery Policy and other Common and Federal Bridge policy changes	Correct minor errors and maintain compliance with Fed PKI (through 2018-06)
3	February 28, 2019	Daniel Wood	Updated based on Comments from BFS	Maintain conformance with FBCA CP
3.1	October 30, 1, 2019	Daniel Wood	Updated Section 5.8 with new language to cover CA terminations	Maintain conformance with Federal/Common CPs
3.2	December 15, 2020	Daniel Wood	Updates in sections: 1, 1.1.1, 1.2, 1.4.1, 2.2.1, 4.4.2, 5.2.1, 5.2.1.1, 5.2.1.2, 5.3.1, 5.3.2, 5.3.7, 5.4.2, 5.5.1, and 6.1.5	Responses to audit findings, annual review findings, change proposals, and for separation of Key Recovery roles from clearance requirements on CA roles
3.3	March 29, 2021 - Not Signed - Not Released	Daniel Wood	Removed the "offline" requirement on OLT Root CAs in section 1.3.1.2 of Addendum 1. Added Addendum 2 – Implementation of PKI Certificates on Treasury Systems	To allow for remote administration on an OLT Root CA, and to define implementation policies on SSL/TLS certificates for HTTPS
3.4	April 27, 2021	Daniel Wood	Punctuation & spelling updates throughout	Final editing for signature & release
3.5	December 7, 2021	Daniel Wood	Rebuilt Doc to eliminate file corruption & formatting issues, and updates in sections: 1, 1.1, 1.2, 1.3.4, 1.3.5, 4.6.6, 4.7.6, 4.8.6, 5.1.2, 5.2.1, 6.4.3, and Addendums 1 & 2	Remove OLT & certificate implementation Addendums (and references to them) to maintain in separate policy doc; Improve descriptions of DDS & Key Recovery roles; Improve cert publishing language; and remove unnecessary requirement on CMS activation data
3.6	December 1, 2022	Daniel Wood	Updates in sections: 1.3.4, 5.1.1, 5.2.1.2, and Appendix B	Response to Auditor recommendations and implementation of FBCA CP Change Proposal 2022-02

## Table of Contents

1.	INTRODUCTION .....	13
1.1	OVERVIEW .....	14
1.1.1	Certificate Policy (CP).....	14
1.1.2	Relationship between the DoT PKI CP and the Dot PKI CA CPSs .....	14
1.1.3	Relationship between the DoT PKI CP and the FBCA and Other Entity CPs.....	14
1.1.4	Scope .....	15
1.1.5	Interaction with PKIs External to the Federal Government.....	16
1.2	DOCUMENT IDENTIFICATION.....	16
1.3	PKI ENTITIES.....	17
1.3.1	Treasury PKI Program Team.....	17
1.3.2	Registration Authority.....	19
1.3.3	Subscribers.....	20
1.3.4	Key Recovery Authorities.....	20
1.3.5	Key Recovery Requestors .....	21
1.3.6	Relying Parties .....	21
1.3.7	Other Participants .....	22
1.4	CERTIFICATE USAGE.....	22
1.4.1	Appropriate Certificate Uses .....	22
1.4.2	Prohibited Certificate Uses .....	24
1.5	POLICY ADMINISTRATION.....	24
1.5.1	Organization Administering the Document.....	24
1.5.2	Contact Person .....	24
1.5.3	Person Determining CPS Suitability for the Policy .....	24
1.5.4	CPS Approval Procedures .....	25
1.6	DEFINITIONS AND ACRONYMS .....	25
2.	PUBLICATION AND REPOSITORY RESPONSIBILITIES .....	26
2.1	REPOSITORIES.....	26
2.2	PUBLICATION OF CERTIFICATION INFORMATION .....	26
2.2.1	Publication of Certificates and Certificate Status .....	26
2.2.2	Publication of CA Information .....	27
2.2.3	Interoperability.....	27
2.3	FREQUENCY OF PUBLICATION.....	27

**UNCLASSIFIED**

- 2.4 ACCESS CONTROLS ON REPOSITORIES..... 27
- 3. IDENTIFICATION AND AUTHENTICATION ..... 28
  - 3.1 NAMING..... 28
    - 3.1.1 Types of Names ..... 28
    - 3.1.2 Need for Names to Be Meaningful..... 32
    - 3.1.3 Anonymity or Pseudonymity of Subscribers..... 33
    - 3.1.4 Rules for Interpreting Various Name Forms..... 33
    - 3.1.5 Uniqueness of Names ..... 33
    - 3.1.6 Recognition, Authentication, and Role of Trademarks..... 33
  - 3.2 INITIAL IDENTITY VALIDATION..... 33
    - 3.2.1 Method to Prove Possession of Private Key..... 34
    - 3.2.2 Authentication of Organization Identity..... 34
    - 3.2.3 Authentication of Individual Identity ..... 35
    - 3.2.4 Non-verified Subscriber Information ..... 39
    - 3.2.5 Validation of Authority ..... 39
    - 3.2.6 Criteria for Interoperation ..... 40
  - 3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS ..... 40
    - 3.3.1 Identification and Authentication for Routine Re-key..... 40
    - 3.3.2 Identification and Authentication for Re-key after Revocation ..... 42
  - 3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST ..... 42
- 4. CERTIFICATE LIFE-CYCLE..... 43
  - 4.1 APPLICATION..... 43
    - 4.1.1 Submission of Certificate Application ..... 43
    - 4.1.2 Enrollment Process and Responsibilities ..... 43
  - 4.2 CERTIFICATE APPLICATION PROCESSING..... 43
    - 4.2.1 Performing Identification and Authentication Functions..... 43
    - 4.2.2 Approval or Rejection of Certificate Applications ..... 44
    - 4.2.3 Time to Process Certificate Applications ..... 44
  - 4.3 ISSUANCE..... 45
    - 4.3.1 CA Actions During Certificate Issuance..... 45
    - 4.3.2 Notification to Subscriber of Certificate Issuance ..... 45
  - 4.4 ACCEPTANCE..... 45
    - 4.4.1 Conduct Constituting Certificate Acceptance..... 45

**UNCLASSIFIED**

- 4.4.2 Publication of the Certificate by the CA ..... 45
- 4.4.3 Notification of Certificate Issuance by the CA to Other Entities ..... 46
- 4.5 KEY PAIR AND CERTIFICATE USAGE ..... 46
  - 4.5.1 Subscriber Private Key and Certificate Usage..... 46
  - 4.5.2 Relying Party Public key and Certificate Usage..... 46
- 4.6 CERTIFICATE RENEWAL ..... 46
  - 4.6.1 Circumstance for Certificate Renewal..... 46
  - 4.6.2 Who May Request Renewal..... 47
  - 4.6.3 Processing Certificate Renewal Requests..... 47
  - 4.6.4 Notification of New Certificate Issuance to Subscriber..... 47
  - 4.6.5 Conduct Constituting Acceptance of a Renewal Certificate..... 47
  - 4.6.6 Publication of the Renewal Certificate by the CA..... 47
  - 4.6.7 Notification of Certificate Issuance by the CA to Other Entities ..... 47
- 4.7 CERTIFICATE RE-KEY..... 47
  - 4.7.1 Circumstance for Certificate Re-key ..... 47
  - 4.7.2 Who May Request Certification of a New Public Key..... 47
  - 4.7.3 Processing Certificate Re-keying Requests..... 48
  - 4.7.4 Notification of New Certificate Issuance to Subscriber ..... 48
  - 4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate..... 48
  - 4.7.6 Publication of the Re-keyed Certificate by the CA..... 48
  - 4.7.7 Notification of Certificate Issuance by the CA to Other Entities ..... 48
- 4.8 MODIFICATION..... 48
  - 4.8.1 Circumstance for Certificate Modification..... 48
  - 4.8.2 Who May Request Certificate Modification..... 49
  - 4.8.3 Processing Certificate Modification Requests ..... 49
  - 4.8.4 Notification of New Certificate Issuance to Subscriber ..... 49
  - 4.8.5 Conduct Constituting Acceptance of Modified Certificate..... 49
  - 4.8.6 Publication of the Modified Certificate by the CA..... 49
  - 4.8.7 Notification of Certificate Issuance by the CA to Other Entities ..... 49
- 4.9 CERTIFICATE REVOCATION AND SUSPENSION..... 50
  - 4.9.1 Circumstances for Revocation ..... 50
  - 4.9.2 Who Can Request Revocation ..... 51
  - 4.9.3 Procedure for Revocation Request..... 51

**UNCLASSIFIED**

- 4.9.4 Revocation Request Grace Period..... 52
- 4.9.5 Time within which CA must Process the Revocation Request..... 52
- 4.9.6 Revocation Checking Requirements for Relying Parties..... 52
- 4.9.7 CRL Issuance Frequency..... 53
- 4.9.8 Maximum Latency of CRLs..... 53
- 4.9.9 On-line Revocation/Status Checking Availability..... 53
- 4.9.10 On-line Revocation Checking Requirements..... 54
- 4.9.11 Other Forms of Revocation Advertisements Available..... 54
- 4.9.12 Special Requirements Related To Key Compromise..... 54
- 4.9.13 Circumstances for Suspension..... 55
- 4.9.14 Who Can Request Suspension..... 55
- 4.9.15 Procedure for Suspension Request..... 55
- 4.9.16 Limits on Suspension Period..... 55
- 4.10 CERTIFICATE STATUS SERVICES..... 55
  - 4.10.1 Operational Characteristics..... 56
  - 4.10.2 Service Availability..... 56
  - 4.10.3 Optional Features..... 56
- 4.11 END OF SUBSCRIPTION..... 56
- 4.12 KEY ESCROW AND RECOVERY..... 56
  - 4.12.1 Key Escrow and Recovery Policy and Practices..... 56
  - 4.12.2 Session Key Encapsulation and Recovery Policy and Practices..... 56
- 5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS..... 57
  - 5.1 PHYSICAL CONTROLS..... 57
    - 5.1.1 Site Location and Construction..... 57
    - 5.1.2 Physical Access..... 57
    - 5.1.3 Power and Air Conditioning..... 59
    - 5.1.4 Water Exposures..... 59
    - 5.1.5 Fire Prevention and Protection..... 59
    - 5.1.6 Media Storage..... 59
    - 5.1.7 Waste Disposal..... 60
    - 5.1.8 Off-Site Backup..... 60
  - 5.2 PROCEDURAL CONTROLS..... 60
    - 5.2.1 Trusted Roles..... 60

**UNCLASSIFIED**

- 5.2.2 Number of Persons Required per Task..... 62
- 5.2.3 Identification and Authentication for Each Role..... 62
- 5.2.4 Separation of Roles..... 63
- 5.3 PERSONNEL CONTROLS..... 63
  - 5.3.1 Background, Qualifications, Experience, and Security Clearance Requirements ..... 63
  - 5.3.2 Background Check Procedures ..... 64
  - 5.3.3 Training Requirements..... 64
  - 5.3.4 Retraining Frequency and Requirements ..... 65
  - 5.3.5 Job Rotation Frequency and Sequence ..... 65
  - 5.3.6 Sanctions for Unauthorized Actions ..... 65
  - 5.3.7 Independent Contractor Requirements ..... 65
  - 5.3.8 Documentation Supplied to Personnel ..... 65
- 5.4 AUDIT LOGGING PROCEDURES..... 66
  - 5.4.1 Types of Events Recorded..... 66
  - 5.4.2 Frequency of Processing Log..... 71
  - 5.4.3 Retention Period for Audit Log ..... 72
  - 5.4.4 Protection of Audit Log ..... 72
  - 5.4.5 Audit Log Backup Procedures..... 73
  - 5.4.6 Audit Collection System (Internal vs. External)..... 73
  - 5.4.7 Notification to Event-Causing Subject..... 73
  - 5.4.8 Vulnerability Assessments ..... 73
- 5.5 RECORDS ARCHIVE ..... 73
  - 5.5.1 Types of Events Archived..... 73
  - 5.5.2 Retention Period for Archive..... 75
  - 5.5.3 Protection of Archive ..... 75
  - 5.5.4 Archive Backup Procedures..... 75
  - 5.5.5 Requirements for Time-Stamping of Records..... 76
  - 5.5.6 Archive Collection System (Internal or External)..... 76
  - 5.5.7 Procedures to Obtain and Verify Archive Information..... 76
- 5.6 KEY CHANGEOVER..... 76
- 5.7 COMPROMISE AND DISASTER RECOVERY..... 77
  - 5.7.1 Incident and Compromise Handling Procedures..... 77
  - 5.7.2 Computing Resources, Software, and/or Data Are Corrupted..... 77

**UNCLASSIFIED**

5.7.3	Entity (CA) Procedures .....	78
5.7.4	Business Continuity Capabilities after a Disaster .....	78
5.8	CA & RA TERMINATION .....	79
6.	TECHNICAL SECURITY CONTROLS.....	81
6.1	KEY PAIR GENERATION AND INSTALLATION.....	81
6.1.1	Key Pair Generation.....	81
6.1.3	Public Key Delivery to Certificate Issuer .....	82
6.1.4	CA Public Key Delivery to Relying Parties.....	83
6.1.5	Key Sizes .....	83
6.1.6	Public Key Parameters Generation and Quality Checking.....	84
6.1.7	Key Usage Purposes (as per X.509 v3 Key Usage Field) .....	84
6.2	PRIVATE KEY PROTECTION & CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS.....	85
6.2.1	Cryptographic Module Standards and Controls.....	85
6.2.2	Private Key Multi-Person Control.....	86
6.2.3	Private Key Escrow .....	87
6.2.4	Private Key Backup.....	87
6.2.5	Private Key Archival.....	88
6.2.6	Private Key Transfer into or from a Cryptographic Module .....	88
6.2.7	Private Key Storage on Cryptographic Module.....	89
6.2.8	Method of Activating Private Keys .....	89
6.2.9	Method of Deactivating Private Keys.....	89
6.2.10	Method of Destroying Private Keys.....	89
6.2.11	Cryptographic Module Rating.....	90
6.3	OTHER ASPECTS OF KEY MANAGEMENT .....	90
6.3.1	Public Key Archival .....	90
6.3.2	Certificate Operational Periods and Key Usage Periods .....	90
6.4	ACTIVATION DATA.....	91
6.4.1	Activation Data Generation and Installation .....	91
6.4.2	Activation Data Protection.....	91
6.4.3	Other Aspects of Activation Data .....	91
6.5	COMPUTER SECURITY CONTROLS.....	92
6.5.1	Specific Computer Security Technical Requirements.....	92
6.5.2	Computer Security Rating.....	93

**UNCLASSIFIED**

- 6.6 LIFE CYCLE TECHNICAL CONTROLS ..... 93
  - 6.6.1 System Development Controls ..... 93
  - 6.6.2 Security Management Controls ..... 94
  - 6.6.3 Life Cycle Security Controls..... 94
- 6.7 NETWORK SECURITY CONTROLS..... 94
- 6.8 TIME STAMPING ..... 94
- 7. CERTIFICATE, CARL/CRL, AND OCSP PROFILES FORMAT ..... 95
  - 7.1 CERTIFICATE PROFILE..... 95
    - 7.1.1 Version Numbers ..... 95
    - 7.1.2 Certificate Extensions ..... 95
    - 7.1.3 Algorithm Object Identifiers..... 95
    - 7.1.4 Name Forms..... 96
    - 7.1.5 Name Constraints..... 97
    - 7.1.6 Certificate Policy Object Identifier..... 97
    - 7.1.7 Usage of Policy Constraints Extension ..... 97
    - 7.1.8 Policy Qualifiers Syntax and Semantics ..... 97
    - 7.1.9 Processing Semantics for the Critical Certificate Policies Extension ..... 97
    - 7.1.10 Key Usage Constraints for id-fpki-common-authentication ..... 97
  - 7.2 CRL PROFILE ..... 97
    - 7.2.1 Version Numbers ..... 97
    - 7.2.2 CRL Entry Extensions..... 97
  - 7.3 OCSP PROFILE..... 98
    - 7.3.1 Version Numbers ..... 98
    - 7.3.2 OCSP Extensions ..... 98
- 8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS..... 99
  - 8.1 FREQUENCY OF AUDIT OR ASSESSMENTS..... 99
  - 8.2 IDENTITY & QUALIFICATIONS OF ASSESSOR..... 99
  - 8.3 ASSESSOR’S RELATIONSHIP TO ASSESSED ENTITY ..... 99
  - 8.4 TOPICS COVERED BY ASSESSMENT..... 100
  - 8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY..... 100
  - 8.6 COMMUNICATION OF RESULTS..... 100
- 9. OTHER BUSINESS & LEGAL MATTERS..... 101
  - 9.1 FEES ..... 101
    - 9.1.1 Certificate Issuance/Renewal Fees..... 101

**UNCLASSIFIED**

9.1.2	Certificate Access Fees.....	101
9.1.3	Revocation or Status Information Access Fee .....	101
9.1.4	Fees for other Services.....	101
9.1.5	Refund Policy.....	101
9.2	FINANCIAL RESPONSIBILITY.....	101
9.2.1	Insurance Coverage.....	101
9.2.2	Other Assets.....	101
9.2.3	Insurance/Warranty Coverage for End-Entities.....	101
9.3	CONFIDENTIALITY OF BUSINESS INFORMATION.....	102
9.3.1	Scope of Confidential Information .....	102
9.3.2	Information not within the Scope of Confidential Information .....	102
9.3.3	Responsibility to Protect Confidential Information.....	102
9.4	PRIVACY OF PERSONAL INFORMATION.....	102
9.4.1	Privacy Plan.....	102
9.4.2	Information Treated as Private.....	102
9.4.3	Information not Deemed Private.....	102
9.4.4	Responsibility to Protect Private Information .....	103
9.4.5	Notice and Consent to Use Private Information .....	103
9.4.6	Disclosure Pursuant to Judicial/Administrative Process.....	103
9.4.7	Other Information Disclosure Circumstances.....	103
9.5	INTELLECTUAL PROPERTY RIGHTS.....	103
9.6	REPRESENTATIONS & WARRANTIES.....	103
9.6.1	CA Representations and Warranties.....	104
9.6.2	Registration Authority Representations and Warranties.....	104
9.6.3	Subscriber Representations and Warranties.....	105
9.6.4	Relying Parties Representations and Warranties.....	105
9.6.5	Representations and Warranties of Other Participants.....	106
9.7	DISCLAIMERS OF WARRANTIES.....	106
9.8	LIMITATIONS OF LIABILITY.....	106
9.9	INDEMNITIES.....	106
9.10	TERM AND TERMINATION .....	106
9.10.1	Term.....	106
9.10.2	Termination .....	106

**UNCLASSIFIED**

9.10.3	Effect of Termination and Survival .....	106
9.11	INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS.....	107
9.12	AMENDMENTS.....	107
9.12.1	Procedure for Amendment .....	107
9.12.2	Notification Mechanism and Period .....	107
9.12.3	Circumstances under which OID must be Changed.....	107
9.13	DISPUTE RESOLUTION PROVISIONS.....	107
9.14	GOVERNING LAW.....	108
9.15	COMPLIANCE WITH APPLICABLE LAW.....	108
9.16	MISCELLANEOUS PROVISIONS.....	108
9.16.1	Entire Agreement.....	108
9.16.2	Assignment .....	108
9.16.3	Severability .....	108
9.16.4	Enforcement (Attorney Fees/Waiver of Rights).....	108
9.16.5	Force Majeure .....	108
9.17	OTHER PROVISIONS.....	108
APPENDIX A	Use of Common Policy Framework OIDS in Federal Legacy PIV Cards .....	109
APPENDIX B	PIV-Interoperable Smart Card Requirements.....	110
APPENDIX C	PIV-I Card Management System Requirements.....	112
APPENDIX D	Summary of Available Policies .....	113
APPENDIX E	BIBLIOGRAPHY.....	116
APPENDIX F	ACRONYMS AND ABBREVIATIONS.....	118
APPENDIX G	GLOSSARY .....	120
APPENDIX H	ACKNOWLEDGEMENTS.....	129

## 1. INTRODUCTION

**Note: The term “policy” is used in this document in the context of X.509 Certificate Policy (CP) as opposed to how the term “policy” is generally used at the Department of the Treasury.**

The United States Department of the Treasury has implemented a Public Key Infrastructure (PKI) that provides a method for securing transmission of information across Department Automated Information System (AIS) assets, and supports the verification of an individual’s identity for physical and logical access control. Overall, the PKI Program establishes a secure electronic environment, at the Controlled Unclassified Information (CUI) level, that fully complements hard-copy documentation standards currently in use. This Certificate Policy (CP) defines the minimum standards necessary to implement and manage the PKI architecture, identifies a PKI Program Team, and details the Department’s program.

A PKI consists of products and services that provide and manage X.509 certificates for public key cryptography. Public key cryptography is an information technology security service that can provide identity authentication, data integrity, technical non-repudiation, and confidentiality (i.e., privacy) to electronic transactions.

This CP defines policies across six different assurance levels under the Treasury Root CA (TRCA): Rudimentary, Basic, Medium, Personal Identity Verification Interoperability (PIV-I) Card Authentication, Medium Hardware, and High. The level of assurance refers to the strength of the binding between the public key and the individual whose subject name is cited in the certificate, the mechanisms used to control the use of the private key, and the security provided by the PKI itself.

Note that the Treasury PKI will also issue certificates with OIDs that correspond to a specific level of assurance established by Federal Common Policy Framework (FCPF) for use in Personal Identity Verification (PIV) cards in compliance with Federal PKI policies (see Appendix A).

In addition, Treasury provides services to other Federal agencies under a Federal Shared Service Provider (SSP) Program. PKI services provided to those agencies are not subject to this CP. SSP CAs serving those agencies operate under the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework (COMMON CP).

All subordinate CA certificates contain at least one NIST-registered Certificate Policy Object Identifier (OID), which a Relying Party may use to decide whether a certificate is trusted for a particular purpose. The OID corresponds to a specific level of assurance established by this CP.

Each end-entity or subordinate certificate issued by the Department will assert the appropriate levels of assurance in the certificate Policies extension. Any use of or reference to this CP outside the purview of the Department of the Treasury PKI Policy Management Authority (PMA) is completely at the using party’s risk. An Entity outside the Department of the Treasury shall not assert the Treasury PKI CP OIDs in any certificates the Entity CA issues, except in the policy Mappings extension establishing an equivalency between a Treasury PKI CP OID and an OID in that Entity CA’s CP.

This CP is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (PKIX) RFC 3647, “Certificate Policy and Certification Practices Framework.” Users shall interpret the terms and provisions of this CP under and be governed by applicable Federal law. This policy is also in consonance

with and augments the information system security requirements in Treasury Department Publication (TD P) 85-01, "Treasury IT Security Program".

The reliability of the public key cryptography portion of the security solution is a direct result of the secure and trustworthy operation of an established PKI, including equipment, facilities, personnel, and procedures. This CP applies to all the components of the Treasury PKI (TPKI).

## **1.1 OVERVIEW**

### **1.1.1 Certificate Policy (CP)**

The United States Department of the Treasury Public Key Infrastructure X.509 Certificate Policy (Treasury PKI CP) is the policy under which the Department establishes and operates the Treasury Root Certification Authority (TRCA) and any subordinate Certification Authorities (CA). The CP defines six distinct assurance levels for use by the Treasury PKI CAs under the TRCA. Relying Parties may wish to base their trust in a given level of assurance on the following:

- Amount and type of inherent risk of an activity
- Consequence of failure
- Use of risk mitigation controls

This document does not define certificate policy for CAs operated by external entities that communicate with the Department, and who issue their own certificates.

In addition, this document defines the creation and management of X.509, version 3, public key certificates for use in applications requiring trusted communication between networked computer-based systems. Such applications include, but are not limited to the following examples: electronic mail; transmission of CUI and/or classified information on the appropriate networks, signature of electronic forms; contract submission signatures; and authentication of infrastructure components such as web servers, firewalls, directories, and mobile code. The Department of the Treasury also issues PKI certificates and provides certificate validation services to authenticate the personal identity of Department employees, contractors, and other affiliated personnel for access to U.S. Government facilities and information systems by means of the PIV credential.

### **1.1.2 Relationship between the DoT PKI CP and the DoT PKI CA CPSs**

The Department of the Treasury PKI X.509 CP states what Subscribers can expect from a certificate issued by the TPKI. The Department of the Treasury CAs' Certification Practices Statements (CPSs) state how Root and subordinate CAs meet those expectations.

### **1.1.3 Relationship between the DoT PKI CP and the FBCA and Other Entity CPs**

This CP applies to certificates issued to CAs, devices, and Federal employees, contractors, and other affiliated personnel. This CP also applies to certificates issued to organizations and/or groups of people, with the understanding that such certificates, by the nature of their issuance and use, cannot support technical non-repudiation.

## UNCLASSIFIED

The TPki exists to facilitate trusted electronic business transactions for Treasury organizations and its affiliates. Programs that carry out or support this mission require services such as authentication, confidentiality, data-integrity, technical non-repudiation, and logical access control. An array of network security components, such as workstations, guards, firewalls, routers, and trusted database servers, satisfy these service requirements. The use of public key cryptography supports and complements the operation of these components. This CP implements a level of assurance comparable to the X.509 Certificate Policy for the Federal Bridge Certificate Authority (FBCA CP) High Assurance Policy and all lower assurance levels. Services provided by the PKI include:

- Key Generation/Storage/Recovery
- Certificate Generation, Update (i.e., Key Recovery), Renewal, Re-key, and Distribution
- Certificate Revocation List (CRL) and Authority Revocation List (ARL) Generation and Distribution
- Directory Management of certificate related items
- Certificate token initialization/programming/management
- System Management Functions (e.g., security audit, configuration management, archive)
- Defining requirements on PKI activities, including the following, ensures the security of these services:
  - Subscriber identification and authorization verification
  - Control of computer and cryptographic systems Operation of computer and cryptographic systems
  - Usage of keys and public key certificates by Subscribers
  - Definition of rules to limit liability and to provide a high degree of certainty

### 1.1.4 Scope

The Federal PKI Policy Authority (FPKIPA) maps levels of assurance between the FBCA and various Entity CAs to facilitate interoperability. Because Treasury is a Federal Legacy PKI, its CP is mapped against that of the FBCA. However, for technical reasons the FPKIPA and Treasury have agreed to issue the actual cross certificates between Treasury and the FBCA. This approach simplifies the certificate path for Treasury's SSP and PIV card programs.

The Treasury PKI X.509 CP is consistent with the FBCA CP and applicable portions of the COMMON CP for all certificate policies that are either directly asserted or mapped to the Federal policies.

In the same manner that the FPKIPA maps the FBCA CP to the Treasury PKI X.509 CP, the Treasury PMA maps other Entity CPs to the levels of assurance in the Treasury PKI X.509 CP. The PMA will approve the acceptance of external CPs for cross certification to the Department of the Treasury TRCA, based on the recommendations of the PKI Operating Authority, the PKI Program Management Office, and any respective assurance mapping levels determined by the FPKIPA. The Department of the Treasury TRCA asserts the relationship between these CPs and the CA in the policyMappings extension of the CA certificates issued by the TRCA. The only exception to this rule is the relationship between the Treasury PKI X.509 CP and those of other Entities that are also cross certified with the FBCA. The Treasury PMA will generally accept the assurance level mapping determinations of the FPKIPA.

Treasury reserves the right to establish locally trusted certificate policies to meet its needs.

**1.1.5 Interaction with PKIs External to the Federal Government**

The Treasury TRCA achieves interoperability with non-Federal CAs that issue under different policies by policy mapping and cross certification through the FBCA, the FCPCA, or directly with the organization in question. The TRCA will extend interoperability with non-Federal entities only when it is beneficial to the Federal Government and to the mission of the Department.

**1.2 DOCUMENT IDENTIFICATION**

The official title of this CP is the U.S. Department of the Treasury Public Key Infrastructure X.509 Certificate Policy. The TRCA operates at six (6) levels of assurance and is authorized to assert certificate policies, at each level, to specify the intended purpose of the certificate. Each policy has a corresponding policy Object Identifier (OID) asserted in certificates issued by CAs within the TPki. The National Institute of Standards and Technology (NIST) assigned the following IETF notation arc for Treasury CPs: 2.16.840.1.101.3.2.1.5.

International Organization for Standardization (ISO) notation represents this as:

treasury-policies OBJECT IDENTIFIER: = {joint-iso-ccitt (2) country (16) us (840)

organization (1) gov (101) csor (3) pki (2) cert-policy (1) treasury-policies (5) [X]}

The Department has registered the following certificate policies in the NIST Computer Security Objects Registry under this arc:

**TABLE 1-1, CERTIFICATE POLICY OIDS**

Certificate Policy	OID suffix	Level of Assurance
treasury-level 1 (Rudimentary)	::= {2 16 840 1 101 3 2 1 5 2}	Rudimentary
treasury-level 2 (Basic - Individual)	::= {2 16 840 1 101 3 2 1 5 3}	Basic
treasury-level 2 (Basic - Organizational)	::= {2 16 840 1 101 3 2 1 5 8}	Basic
treasury-level 3 (Medium H/W)	::= {2 16 840 1 101 3 2 1 5 4}	Medium Hardware
treasury-level 5 (High H/W)	::= {2 16 840 1 101 3 2 1 5 5}	High
treasury-level 7 (Medium S/W)	::= {2 16 840 1 101 3 2 1 5 7}	Medium
treasury-pivi-hardware (PIV-I Hardware)	::= {2 16 840 1 101 3 2 1 5 10}	Medium Hardware
treasury-pivi-cardAuth (PIV-I Card Authentication)	::= {2 16 840 1 101 3 2 1 5 11}	PIV-I Card Authentication
treasury-pivi-contentSigning (PIV-I Content Signing)	::= {2 16 840 1 101 3 2 1 5 12}	Medium Hardware

The appropriate TRCA or subordinate CA CPS specifies which policy OIDs that CA asserts. Federal PKI policy reserves the High Assurance policy for U.S. Federal government entity PKI operation and use.

The PIV-I Content Signing policy is reserved for certificates used by the Card Management System (CMS) to sign the PIV-I card security objects. All other device certificates shall assert the COMMON CP Common-Device or Common-Device-Hardware Policy OIDs.

## 1.3 PKI ENTITIES

### 1.3.1 Treasury PKI Program Team

#### *1.3.1.1 Treasury PMA*

The Treasury PMA resides in the Office of the Chief Information Officer (OCIO) for the Department of the Treasury. The PMA provides management authority over the Department's PKI and SSP program. As such, the PMA ensures the conformity to central Department policy for PKI implementation and operation to ensure installation of one PKI solution throughout the Department.

In addition the PMA has established a management body for the agencies that operate under the SSP. This body consists of individuals who have the responsibility for overseeing policies of their CAs. The Treasury PMA is responsible for:

- The Treasury CP.
- Review, approval, and compliance review of all Treasury CPSs issued and maintained in support of the TPKE.
- Approval of any subordinate or other certificate authorities created in support of other Agencies and Bureaus to support digital technologies for authentication, signing, encryption, access, or authorizations.
- Oversight compliance management of the TPKE and all Treasury CAs signed by the TRCA.
- Internal Auditing and compliance oversight of TPKE operations.
- Determinations regarding CP and CPS compliance and assurance level with the Department of the Treasury CP.
- Review and approval of Treasury or other Entities CPs and CPSs pertaining to CAs being considered for cross certification with the TRCA.
- Notifying its customer Agencies and the FPKIPA of any change to the infrastructure that has the potential to affect the FPKI operational environment at least two weeks prior to implementation.

In the event the PMA makes the determination that other, non-Department of the Treasury Certificate Policies offer appropriately equivalent levels of assurance to the Department of the Treasury Certificate Policies. The TPKE may respond to such decisions by methods including but not limited to the following:

- Issuing cross certificates to other PKIs asserting other policies
- Including certificates issued by other PKIs and asserting other Certificate Policies, in Department of the Treasury Certificate Status Authorities (CSAs)
- Recommending CAs asserting other Certificate Policies for inclusion in Department of the Treasury application trust lists

## UNCLASSIFIED

The PMA shall make information regarding such equivalency determinations widely available to Department of the Treasury Subscribers and Relying Parties.

### **1.3.1.2 TRCA**

The TRCA (the collection of hardware, software, and operating personnel) is established by the Program Management Office (PMO) to certify subordinate CAs that, in turn, create, sign, and issue public key certificates to subscribers within Treasury and other related PKI communities. The Department's PKI operates in a hierarchical fashion, utilizing a TRCA and subordinate CAs. The TRCA serve as the trust anchors for all certificates issued under this policy. The TRCA also acts as the Principal CA (PCA) for Treasury to cross certify directly with the Federal PKI (e.g., through the exchange of cross certificates).

The PCA issues either end entity certificates, or CA certificates to other Entity or external party CAs, or both. The PCA shall cross certify with the FCPCA, and other root level CAs from other trust domains as appropriate. Prior to issuing a cross certificate to another root level domain CA, the PCA shall ensure that the new cross certificate does not result in multiple paths to a CA already participating in the FPKI. The PCA shall also certify CA's within Treasury that want to be part of the subordination hierarchy (as opposed to cross certification).

This policy permits an off-line TRCA. The TRCA shall be physically isolated from all networks. The TRCA is responsible for issuing and managing certificates; and ensuring that the performance of all aspects of CA services, operations, and infrastructure related to certificates issued under this policy are in accordance with the requirements, representations, and warranties of this policy. This includes the following:

- The TRCA certifies subordinate CAs, which will assert one or more assurance levels defined in this CP, and outlined in the appropriate CPS
- The TRCA shall also comply with the requirements set forth in applicable Memorandum of Agreement (MOA), Memorandum of Understanding (MOU), and contractual agreements with cross certified CAs and/or other entities

### **1.3.1.3 Subordinate Certification Authorities**

Subordinate CAs are responsible for all aspects of the issuance and management of a certificate to users and devices, including control over the enrollment process, the identification and authentication process, the certificate manufacturing process, publication of certificates, revocation of certificates, and re-key.

A CA, which issues certificates that assert the policies defined in this document, shall conform to the stipulations of this document, including the following:

- Providing to the appropriate authorities a CPS, as well as any subsequent changes, for conformance assessment
- Maintaining its operations in conformance to the stipulations of the approved CPS
- Ensuring that registration information is accepted only from Registration Authorities (RAs)/Local Registration Authorities (LRAs) who understand and are obligated to comply with this policy, and operating under an approved CPS
- Including only valid and appropriate information in the certificate, and to maintaining evidence that due diligence was exercised in validating the information contained in the certificate

- Ensuring that all Subscribers (government and non-government) are informed of their obligations under Sections 1.4 and 9.6.3, including the consequences of not complying with those obligations, and revoking the certificates of Subscribers found to have acted in a manner counter to those obligations
- Operating or obtaining the services of an online repository that satisfies the obligations under Sections 1, 4.10, 9.6.1 and 9.6.5, and informing the repository service provider of those obligations if applicable

#### ***1.3.1.4 Certificate Status Servers***

The TPKE may optionally include an authority that provides status information about certificates on behalf of the Treasury PKI CAs through online transactions. Examples include Online Certificate Status Protocol (OCSP) responders, termed Certificate Status Servers (CSS) identified in the Authority Information Access (AIA) extension. Where certificates identify the CSS as an authoritative source for revocation information, the operations of that authority are within the scope of this CP. A CSS shall assert all the policy OIDs for which it is authoritative. This policy does not cover OCSP servers that are locally trusted, as described in RFC 2560.

#### ***1.3.1.5 Card Management System***

The TPKE uses CMS to manage smart card token content. It is a required component of the TPKE that issues certificate for PIV-I Identification Cards. The CMS is issued content signing certificates appropriate to the types of Subscriber tokens. It uses the appropriate content signing certificate private key to sign content (e.g., fingerprints) captured from the subscriber and inserted into the token during the issuance process.

The CMS shall not be issued any certificates that express the any policy OID other than the appropriate content signing policy.

### **1.3.2 Registration Authority**

The Treasury Registration Authorities (RA) are entities recognized as authorized to collect and verify users' identity and information which is to be entered into the Subscriber's public key certificates. The key difference between RAs and LRAs is the nature and degree of their respective access to the Treasury PKI CAs. The RA, by definition, functions as the Officer trusted role of the Treasury PKI CA as defined in Section 5.2.1.2. The PMO appoints RA(s) for Treasury TRCA from members of the PMO, PKI Program Team, or other Treasury personnel as necessary for specific operational requirements, and who perform their functions in accordance with a CPS approved by the PMA, as detailed in Section 1.3.1.5.

Both CAs and RAs are termed "Certificate Management Authorities (CMA)." This policy uses the term "CMA" when a function may be assigned to either a CA or an RA, or when a requirement applies to both CAs and RAs. The term RA includes entities such as Local Registration Authorities (LRA), unless otherwise specified. Section 5.2.1, Trusted Roles, lists specifically defined trusted roles, i.e., roles whose incumbents perform functions that involve the handling of sensitive cryptographic material and can thus introduce security problems to the CA if not carried out properly. LRAs are not Officers of the PKI. They act as trusted agents providing support to an RA that performs the Officer trusted role.

## UNCLASSIFIED

The division of Subscriber registration responsibilities between the CA and RA may vary among implementations of this CP, as outlined in the appropriate CPS. All CMAs shall protect personal information from unauthorized disclosure as mandated by the Privacy Act of 1974, as amended.

### **1.3.3 Subscribers**

A Subscriber is the entity (the user to whom, or device to which, a certificate is issued) whose Distinguished Name (DN) appears as the subject in a certificate, and who asserts that it uses the key and certificate in accordance with this policy. Sometimes, a PKI technically considers CAs as "Subscribers." 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. Department of the Treasury PKI Subscribers include but are not limited to the following categories of entities that may wish to conduct official Department business:

- Department of the Treasury personnel: Direct Hire, Part-time/Intermittent/Temporary (PIT) employees, contractors, commercial vendors, and agents
- Federal Government departments and agency personnel, and their contractors and agents
- Workstations, guards and firewalls, routers, trusted servers (e.g., database, domain controller, FTP, and WWW), and other infrastructure components. These components must be under the cognizance of humans, who accept the certificate and are responsible for the correct protection and use of the associated private key

A PKI Sponsor fills the role of a Subscriber for groups, organizations, disabled personnel, and non-human system components named as public key certificate subjects. The PKI Sponsor works with the CMAs to register the above elements in accordance with Section 3.2.2 and 3.2.3 and is responsible for meeting the obligations of Subscribers as defined throughout this document.

TRCA Subscribers include only PMA, PMO or other PKI Program Team personnel and, when determined by the PMA, PKI network or hardware devices.

The Treasury may issue certificates to Subscribers other than employees of the U.S. Government, such as commercial vendors and agents, at the convenience of the Government and without fee, when those Subscribers have a bona fide need to possess a certificate issued by a Treasury CA. The Treasury shall inform such Subscribers of the stipulations of this policy by including the provisions of Section 9.6.3 in the Subscriber agreements. These Subscribers are under the same policy obligations as those specified for a Treasury direct hire.

### **1.3.4 Key Recovery Authorities**

In conformance with the latest version of the FBCA CP, key recoveries associated with policies defined in this CP comply with the FPKI Key Recovery Policy (KRP). This section provides an overview of the Treasury authorities involved in key recovery. Section 5.2.1 includes descriptions of the trusted roles involved in key recovery.

#### ***1.3.4.1 Key Escrow Database***

The Key Escrow Database (KED) maintains and secures the key escrow repository and responds to key recovery requests.

#### ***1.3.4.2 Data Decryption Server***

A Data Decryption Server (DDS) has the capability to recover escrowed private decryption keys from the KED (upon proper validation of a request) for the decryption of data within its secure boundary. A DDS does not provide the keys to the Requestor; it provides the decrypted data. The keys only remain in the DDS temporarily and are not recoverable from the DDS.

#### ***1.3.4.3 Key Recovery Agent***

a Key Recovery Agent (KRA) is an individual who is authorized to recover an escrowed key. KRAs provide recovered keys to the Key Recovery Official (KRO) or directly to the Requestor, or they interact with the Data Decryption Server to authorize the decryption of encrypted data on behalf of a Requestor. The number and location of KRAs should be closely controlled.

#### ***1.3.4.4 Key Recovery Official***

A KRO may optionally be used to support identity verification and authorization validation tasks, for the KRA. KROs do not have privileged access to the KED.

For data decryption, a KRO, is an individual who is authorized to perform identity verification and authentication of Requestors and submit a data recovery request on behalf of Requestors.

### **1.3.5 Key Recovery Requestors**

A Requestor requests the recovery of a private decryption key, or the decryption of encrypted data via the DDS. A Requestor may be the Subscriber named in the certificate associated with the key being recovered, or a third-party Requestor. Any individual who can demonstrate a verifiable authority and a need to obtain a recovered key, or the decryption of encrypted data, may be considered a Requestor.

#### ***1.3.5.1 Internal Third-Party Requestor***

An Internal Third-Party Requestor is any Requestor who is in the Subscriber's supervisory chain or otherwise authorized to obtain the Subscriber's key or decrypt the Subscriber's encrypted data.

#### ***1.3.5.2 External Third-Party Requestor***

An External Third-Party Requestor is someone (e.g., investigator) outside the Issuing Organization with a court order or other legal instrument to obtain the Subscriber's private decryption key or decrypt the Subscriber's encrypted data.

### **1.3.6 Relying Parties**

A Relying Party uses a Subscriber's certificate to verify or establish:

- the identity and status of an individual
- the integrity of a digitally signed message
- the identity of the creator of a message
- confidential communications with the Subscriber

The Relying Party relies on the validity of the binding between the Subscriber's name and public key. A Relying Party may use information in the certificate (such as Certificate Policy Identifiers) to determine the suitability of the certificate for a particular use. The Relying Party is responsible for deciding whether or

how to check the validity of the certificate by checking the appropriate certificate status information. For this Certificate Policy, the relying party may be any Entity that wishes to validate the binding of a public key to the name of a federal employee, contractor, other affiliated personnel, or devise.

This CP makes no assumptions or limitations regarding the identity of Relying Parties. While Relying Parties may be Subscribers, Relying Parties are not required to have an established relationship with the Treasury PKI CA, FBCA, or another Entity CA.

### **1.3.7 Other Participants**

All CAs operating under this policy require the services of other security and application authorities, such as compliance auditors and attribute authorities. Each CA shall identify, in its CPS, the parties responsible for providing such services and the mechanisms used to support these services. Section 5.2 provides more detail on these authorities, services, and mechanisms.

## **1.4 CERTIFICATE USAGE**

### **1.4.1 Appropriate Certificate Uses**

The sensitivity of the information processed or protected using certificates issued by the TPKE may vary significantly. Relying Parties should evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. Each Relying Party makes this evaluation for its application outside the control of this CP. To provide sufficient granularity, this CP specifies security requirements at six increasing, qualitative levels of assurance (Rudimentary, Basic, Medium, PIV-I Card Authentication, Medium Hardware, and High), and a separate assurance level for Internal OLT defined in Addendum 1.

All Treasury bureaus that use PKI technology to secure data are subject to the requirements of this policy. The TPKE is intended to support applications involving unclassified information, which can include CUI data protected pursuant to Federal statutes and regulations. Other agencies that exchange information electronically with Department assets, including those requiring the security of Public Key technology, are subject to the same requirements. Each CA asserting this policy must state this requirement in the CPS and inform Subscribers of the limitation.

The level of assurance associated with a public key certificate describes the procedures and controls involved in validating a Subscriber's identity and binding that identity to a public key. It is the responsibility of the Relying Party to assess that level of assurance and determine if it meets their security requirements for some particular use. The level of assurance depends on the proper generation and management of the certificate and associated private keys, in accordance with the stipulations of this policy. Personnel, physical, procedural, and technical security controls contribute to the assurance level of the certificates issued by a certificate management authority or system.

The following table provides a brief description of the appropriate uses for certificates at each level of assurance defined in this CP. These descriptions are guidance and are not binding

**UNCLASSIFIED**

**TABLE 1-2, CERTIFICATE USES**

Assurance Level	Appropriate Certificate Uses
Rudimentary	This level provides the lowest degree of assurance concerning identity of the individual. One of the primary functions of this level is to provide data integrity to the digitally signed information. This level is relevant to environments in which the risk of malicious activity is considered low. It is not suitable for transactions requiring authentication, and is generally insufficient for transactions requiring confidentiality, but may be used for the latter where certificates having higher levels of assurance are unavailable.
Basic	This level provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but which are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high. This security level assumes that subscribers are not likely to be malicious.
Medium	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial.
PIV-I Card Authentication	This level is used to uniquely identify a PIV-I card – not the cardholder – for the purposes granting the cardholder physical access to high-volume, low-risk areas or in combination with other authentication mechanisms for access to high-risk areas.
Medium Hardware	This level is relevant to environments where threats to data are high or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.
High	This level is reserved for cross certification with government entities and is appropriate for those environments where the threats to data are high, or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.

General usage for certificates covered by this policy includes:

- Digital signature services (authentication and data integrity)
- Protection (confidentiality)
- Technical non-repudiation
- Authentication of identity and status with the Department for access control to a Federal facility or information systems across the Federal Government

### **1.4.2 Prohibited Certificate Uses**

Subscribers shall not use Treasury PKI certificates to conceal an unauthorized act as specified in Federal law or Department of the Treasury regulations. Examples of such actions include, but are not limited to, the following:

- Use of PKI certificates, especially in conjunction with a Treasury-issued PIV card, to gain unauthorized access to a Federal facility, information system, or electronic data (e.g., Privacy information), or to enable others to gain such access
- Use of PKI certificates to facilitate and/or hide an unauthorized action, such as:
- Transfer information to an unauthorized individual
- Generate income for oneself or for an organization
- View sexually explicit material, gamble, or for the purposes of conducting Unlawful or malicious activities
- Negatively affect the integrity, accessibility, and/or confidentiality of the Department's cyber infrastructure

The Treasury specifically prohibits such uses of PKI regardless of whether the use is during or outside normal work hours, whether use occurs on or off U.S. Government premises, or whether the use occurs within or outside the United States.

Each CA asserting this policy must state this requirement in the CPS and inform Subscribers of these usage limitations. All Departments of the Treasury bureaus, offices, and posts that use PKI technology are subject to the requirements of this policy.

## **1.5 POLICY ADMINISTRATION**

### **1.5.1 Organization Administering the Document**

The PMA is responsible for all aspects of this CP.

### **1.5.2 Contact Person**

Direct questions regarding this CP to Treasury PMA, at the following address:

Daniel W. Wood  
U.S. Department of the Treasury, Suite 12000  
1750 Pennsylvania Ave. N.W., 7730E Washington, DC 20220  
(202) 622-5144  
[Daniel.Wood@Treasury.gov](mailto:Daniel.Wood@Treasury.gov)

### **1.5.3 Person Determining CPS Suitability for the Policy**

Certification Practices Statements, derived from this CP, must conform to the corresponding requirements of this Certificate Policy. The PMA shall determine the suitability of any CPS to this policy. In each case, the PMA shall base the determination of suitability on a compliance audit results and recommendations.

See section 8 for further details.

#### **1.5.4 CPS Approval Procedures**

The Treasury PMO shall submit the CPS for all CAs operated under this policy and the results of the compliance audit(s) to the Treasury PMA. Other entities operating PKI components shall submit a CPS or Key Recovery Practice Statement (KRPS) and the results of the compliance audit(s) to the Treasury PMA.

CAs issuing under this policy and other components of the PKI are required to meet all facets of the policy. The Treasury PMA shall make the determination that a CPS or KRPS complies with this policy. All components of the PKI (e.g., CA, RA) must meet all requirements of an approved CPS or KRPS before commencing operations.

The Treasury PMA shall decide what variations in CMA or Key Recovery practices are acceptable under this CP. A CMA or other component operator may request a permanent change to this CP. Change proposals shall be submitted to the Treasury PMA. When a change proposal is accepted and approved by the Treasury PMA, the Treasury PMO shall post the change proposal on its web site which is accessible by interested or Relying Parties.

The PMA shall notify the FPKIPA, and provide information regarding the specific provision changed, the rationale for the change, and either get approval or a request to submit the Department policy for re-cross certification.

#### **1.6 DEFINITIONS AND ACRONYMS**

See Appendices F and G.

## 2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

### 2.1 REPOSITORIES

The PKI Program Team shall operate repositories to support TPKE CA operations. The location of any publication will be one that is appropriate to the certificate-using community, and in accordance with the total security requirements of the Department. The PKI Program Team shall ensure interoperability with the FBCA repository.

The TPKE CA infrastructure will serve as the primary repository of information for Subscribers and Relying Parties. For all TPKE CAs, this repository is the Treasury directory infrastructure. The PKI Program Team web site (<http://pki.treas.gov>) will serve as the primary repository to publish public information. Network directories and all other repositories used to disseminate relevant information will:

- Maintain availability necessary to distribute current certificate information in a manner consistent with the posting and retrieval stipulations of Section 2.2.1, and the appropriate CA CPS
- Implement access controls on all CA repositories to provide sufficient protection as described in Section 5.1.2

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

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

### 2.2 PUBLICATION OF CERTIFICATION INFORMATION

#### 2.2.1 Publication of Certificates and Certificate Status

TRCA and each subordinate CA in the TPKE shall publish certificates and status information into appropriate repositories. The repositories shall be available such that they are available over the publicly accessible network or other such networks appropriate to a particular "community of interest". The repositories shall contain the following:

- CA certificates (from and to each CA in the TPKE)
- All CRL and ARL (each CA may also utilize an OCSP responder)

The PKI Program Team shall use only repository mechanisms (directory, CSS) and procedures designed to ensure CA certificates and CRLs are available for retrieval 24 hours a day, 7 days a week, with a minimum of 99% availability overall per year and scheduled down-time not to exceed 0.5% annually.

### **2.2.2 Publication of CA Information**

The PKI Program Team shall publish information concerning the Treasury PKI necessary to support its use and operation. The PMO shall publish information (including this policy) on a web site, consistent with Department of the Treasury policies regarding web site contents that is available to Subscribers and Relying Parties. Due to sensitivity, the Department will not publish any Treasury PKI CA CPS.

### **2.2.3 Interoperability**

Where the TPKI publishes certificates and CRLs in directories, the directories shall use standards-based schemas whenever possible for directory objects and attributes in accordance with technical guidance from the FPKI Management Authority (see <http://www.idmanagement.gov/federal-public-key-infrastructure-management-authority>).

## **2.3 FREQUENCY OF PUBLICATION**

The PMA shall make this CP and any subsequent changes publicly available within 30 days of approval. The appropriate Treasury PKI CA will publish certificates following user acceptance as specified in Section

4.4 and proof of possession of private key as specified in Section 3.2.1. Section 4.9 specifies publication

requirements for CRLs. The CA shall publish all information normally published in the repository promptly after such information becomes available. Each PKI CA CPS specifies time limits within which it publishes various types of information.

## **2.4 ACCESS CONTROLS ON REPOSITORIES**

Direct and /or remote access to information in TPKI repositories shall be determined by the PMO pursuant to the rules and statutes that apply. The Treasury PKI PMO shall protect any repository information not intended for public dissemination or modification. Public key certificates and certificate status information in a TPKI repository shall be publicly available through the Internet wherever reasonable. At a minimum, the TPKI repositories shall make CA certificates and CRLs issued by the TPKI and CA certificates issued to the TPKI available to Federal Relying Parties.

The appropriate CPS will detail what information in the repository shall be exempt from automatic availability and to whom, and under what conditions the PMO may make restricted information available.

### 3. IDENTIFICATION AND AUTHENTICATION

#### 3.1 NAMING

##### 3.1.1 Types of Names

All Treasury CAs shall be able to generate and sign certificates that contain an X.501 DN or, if applicable, a Domain Component (DC) identifier.

The TPki was implemented before 2004 and is considered a “Federal Legacy PKI” and therefore may use the existing directory tree schema while in transition to the directory schemas defined below. Common name fields will be populated as specified below for Federal and Contractor employees. For legacy Treasury Subscribers, naming within the certificate will conform to the following:

For Treasury employee Subscribers, the DN will be formatted according to the following:

“CN=userID, OU=bureau, OU=Department of the Treasury, OU=structural container, O=U.S. Government, C=US”

The organizational unit bureau and Department of the Treasury are used to specify the federal entity that employs the subscriber. At least one of these organizational units must appear in the DN. The additional organizational unit structural container is permitted to support local directory requirements, such as differentiation between human subscribers and devices. This organizational unit may not be employed to further differentiate between subcomponents within a bureau.

The userID is unique across the Treasury directory. It is a non-identifying ID and can be composed in the following form: the first two letters of the subscribers’ surname and a four-digit number that is assigned sequentially as userID are assigned. The directory can be queried using a subscriber name (as long as access controls are not in place to protect it) or userID to get the subscriber’s certificate.

For non-human Subscribers, a PKI Sponsor must provide a uniquely identifying name for the entity to be issued a certificate. This information may be a URL, IP address, hostname, application or process name, or other value that can reasonably identify this equipment. The name of the PKI sponsor does not need to appear in the certificate but may be kept as an attribute in the directory. An example of a non-human subject would be:

CN=www.publicdebt.ustreas.gov, OU=Bureau of Public Debt, OU=Department of the Treasury, O=U.S. Government, C=US

For certificates issued under policies associated with Basic, Medium, Medium Hardware, High, and for devices, the TPki shall generate and sign certificates that contain an X.501 DN. These distinguished names may be in either one of two forms: a geo-political name space or an Internet DC name space. Where Subscriber certificate name forms must assert the PIV OIDs, Subscriber DNs shall also meet FCPCA naming policies.

## UNCLASSIFIED

The organizational units department and agency appear when applicable and are used to specify the federal entity that employs the subscriber. At least one of these organizational units must appear in the DN. The additional organizational unit structural container is permitted to support local directory requirements, such as differentiation between human subscribers and devices. This organizational unit may not be employed to further differentiate between subcomponents within an agency.

All geo-political X.501 distinguished names assigned to Federal employees are in one of the following directory information trees:

C=US, o=U.S. Government, [ou=department], [ou=agency], [ou= structural\_container] C=US, [o=department], [ou=agency], [ou= structural\_container]

All certificates issued after May of 2006 shall assign names that conform to the remainder of this section.

The organizational units department and agency appear when applicable and are used to specify the TPKI Sponsor that employs the subscriber. At least one organizational unit must appear in

the DN. The distinguished name of the Federal employee subscriber shall be structured in one of the three following forms:

1. C=US, o=U.S. Government, [ou=department], [ou=agency], [ou= structural\_container],  
cn=nickname lastname
2. C=US, o=U.S. Government, [ou=department], [ou=agency], [ou= structural\_container],  
cn=firstname initial. lastname
3. C=US, o=U.S. Government, [ou=department], [ou=agency], [ou= structural\_container],  
cn=firstname middlename lastname

In the first name form (for both Federal or Contractor employees), nickname may be the subscriber's actual first name, a form of their first name, middle name, or pseudonym (e.g., Chuck for Charles) by which the subscriber is generally known.

X.501 distinguished names assigned to Federal contractors and other affiliated persons shall be within the same directory information tree. The distinguished name of the Federal contractor subscriber and any affiliate subscribers must take one of the three following forms:

1. C=US, o=U.S. Government, [ou=department], [ou=agency], [ou= structural\_container],  
cn=nickname lastname (affiliate)
2. C=US, o=U.S. Government, [ou=department], [ou=agency], [ou= structural\_container],  
cn=firstname initial. lastname (affiliate)
3. C=US, o=U.S. Government, [ou=department], [ou=agency], [ou= structural\_container],  
cn=firstname middlename lastname (affiliate)

Distinguished names based on Internet DC names shall be in one of the following directory information trees:

1. dc=gov, dc=org0, [dc=org1], [ dc=orgN]

## UNCLASSIFIED

2. dc=mil, dc=org0, [dc=org1], [ dc=orgN]

The default Internet domain name for any TPKI participating component using either the [orgN.]...[org0].gov or [orgN.]...[org0].mil branches shall be used to determine DN's uniqueness. The first DC of the DN shall be dc=gov or dc=mil. At a minimum, the org0 DC must appear in the DN. The org1 to orgN DCs appear, in order, when applicable and are used to specify the Treasury entity that employs the subscriber.

The distinguished name of the TPKI Federal employee subscriber must take one of the following three forms when the TPKI Sponsor's Internet domain name ends in .gov:

1. dc=gov, dc=org0, [dc=org1], [dc=orgN], cn=nickname lastname
2. dc=gov, dc=org0, [dc=org1], [dc=orgN], cn=firstname initial. lastname
3. dc=gov, dc=org0, [dc=org1], [dc=orgN], cn=firstname middlename lastname

The distinguished name for Federal contractors and affiliated subscribers must use one of the following three forms when the TPKI Sponsor's Internet domain name ends in .gov:

1. dc=gov, dc=org0, [dc=org1], [dc=orgN], cn=nickname lastname (affiliate)
2. dc=gov, dc=org0, [dc=org1], [dc=orgN], cn=firstname initial. lastname (affiliate)
3. dc=gov, dc=org0, [dc=org1], [dc=orgN], cn=firstname middlename lastname (affiliate)

The distinguished name of the Federal employee subscriber must use one of the following three forms when the TPKI sponsor's Internet domain name ends in .mil:

1. dc=mil, dc=org0, [dc=org1], [dc=orgN], cn=nickname lastname
2. dc=mil, dc=org0, [dc=org1], [dc=orgN], cn=firstname initial. lastname
3. dc=mil, dc=org0, [dc=org1], [dc=orgN], cn=firstname middlename lastname

The distinguished name of the Federal contractors and affiliated subscribers must use one of the following three forms when the TPKI sponsor's Internet domain name ends in .mil:

1. dc=mil, dc=org0, [dc=org1], [dc=orgN], cn=nickname lastname (affiliate)
2. dc=mil, dc=org0, [dc=org1], [dc=orgN], cn=firstname initial. lastname (affiliate)
3. dc=mil, dc=org0, [dc=org1], [dc=orgN], cn=firstname middlename lastname (affiliate)

PIV-I Hardware 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:

cn=Subscriber's full name, ou=Affiliated Organization Name, {Base DN}

For certificates with no Affiliated Organization:

cn=Subscriber's full name, ou=Unaffiliated, ou=Entity CA's Name, {Base DN}

PIV-I Content Signing certificates shall clearly indicate the organization administering the CMS.

## UNCLASSIFIED

For PIV-I Card Authentication subscriber certificates, use of the subscriber common name is prohibited. 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").

The CA may supplement any of the name forms for users specified in this section by including a dnQualifier, serial number, or user id attribute. When any of these attributes are included, they may appear as part of a multi-valued relative distinguished name (RDN) with the common name or as a distinct RDN that follows the RDN containing the common name attribute. Generational qualifiers may optionally be included in common name attributes in distinguished names based on Internet domain names. For names assigned to employees, generational qualifiers may be appended to the common name. For names assigned to federal contractors and other affiliated persons, generational qualifiers may be inserted between lastname and "(affiliate)".

Sponsored devices that are the subject of certificates shall be assigned either a geo-political or an Internet DC name. Device names must use one of the following forms:

1. C=US, o=U.S. Government
2. [ou=department]
3. [ou=agency]
4. cn=device name
5. dc=gov, dc=org0
6. [dc=org1], [dc=orgN]
7. [cn=device name]
8. dc=mil, dc=org0
9. [dc=org1]
10. [dc=orgN]
11. [cn=device name]

Where device name is a descriptive name of the device, and when a device is fully described by the Internet domain name, the common name attribute is optional.

Treasury CAs and CSSs distinguished names shall be either a geo-political or an Internet DC name. The TPKI will use the following naming convention for certificate authorities:

C=US, o=U.S. Government, ou=Department of the Treasury, ou=Certification Authorities, cn= [CA name]

## UNCLASSIFIED

A TPKI participant or sponsoring entity reserves the right to issue certificates using any of the above-defined naming conventions in order to prevent duplication of Subscriber names to maintain uniqueness within the domain.

The table below summarizes the naming requirements that apply to each level of assurance.

**TABLE 3-1, NAMING REQUIREMENTS**

<b>Assurance Level</b>	<b>Naming Requirements</b>
Rudimentary	Non-Null Subject Name, or Null Subject Name if Subject Alternative Name is populated and marked critical
Basic	Non-Null Subject Name, and optional Subject Alternative Name if marked non-critical
Medium (all policies)	Non-Null Subject Name, and optional Subject Alternative Name if marked non-critical
PIV-I Card Authentication	Non-Null Subject Name and Subject Alternative Name
High	Non-Null Subject Name, and optional Subject Alternative Name if marked non-critical

### **3.1.2 Need for Names to Be Meaningful**

Names used within the certificates shall identify the person or object to which assigned in a meaningful way. For equipment, this may be a model name and serial number, or an application process (e.g., Organization X Mail Server). Any CA asserting this policy shall only sign certificates with subject names from within a name-space approved by the PMO and PMA.

The directory information tree must accurately reflect organizational structures. In addition, the common name shall represent the Subscriber in a way that is easily understandable for humans.

The common name within the DN must respect name space uniqueness requirements and must not be misleading. This does not preclude the use of pseudonymous certificates as defined in Section 3.1.3.

When User Principal Names (UPN) are used, they must be unique and accurately reflect organizational structures.

While the issuer name in CA certificates is not generally interpreted by Relying Parties, this CP requires use of meaningful names by CAs issuing under this policy. If included, the common name should describe the issuer, such as:

cn=Treasury Operational CA-1

The subject name in CA certificates must match the issuer name in certificates issued by the subject, as required by RFC 5280.

### **3.1.3 Anonymity or Pseudonymity of Subscribers**

The TRCA shall not issue anonymous certificates. Subordinate CAs may issue pseudonymous certificates to support internal operations. CA certificates issued by the TRCA shall not contain anonymous or pseudonymous identities.

### **3.1.4 Rules for Interpreting Various Name Forms**

Rules for interpreting name forms will use the appropriate standard. Rules for interpreting distinguished name forms are specified in X.501. Rules for interpreting e-mail addresses are specified in [RFC 2822].

Rules for interpreting the UUID name type are specified in RFC 4122.

### **3.1.5 Uniqueness of Names**

The Treasury CMAs must enforce name uniqueness within the X.500 name space, which they have been authorized, and that uniqueness shall be enforced by the PMO under the auspices of the Treasury Office of the CIO. Name uniqueness is not violated when multiple certificates are issued to the same entity. The userID attribute is used to ensure that no two individuals are assigned the same DN, and therefore potentially the same electronic identity or credential.

Each Treasury PKI CA will unambiguously identify each object in the naming hierarchy for the certificate repository using DNs. The Treasury CAs will ensure that a DN, once assigned, remains unique for the lifetime of the PKI, and will not re-use that name to identify a different entity.

When other name forms are used, CMAs must allocate them, to ensure such name uniqueness across the Department. Each Treasury PKI CA shall document in its CPS;

- What name forms shall be used,
- How the TPKI will interact with the enterprise services to ensure this is accomplished, and
- How Treasury will allocate names within the Subscriber community to guarantee name uniqueness among current and past Subscribers (e.g., if “Joe Smith” leaves a CA’s community of Subscribers, and a new, different “Joe Smith” enters the same community of Subscribers, how will these two people be provided unique names?).

The CMA shall investigate and if necessary, recommend the correction for any name collisions brought to its attention. The CMA shall coordinate with and defer to the PMO where appropriate.

### **3.1.6 Recognition, Authentication, and Role of Trademarks**

The CMA shall investigate and if necessary, recommend the correction for any trademark name collisions brought to its attention. The CMA shall coordinate with and defer to the PMO where appropriate. The CMA will communicate resolutions to all interested parties. Consistent with Federal Policy, Treasury PKI CAs will not knowingly use trademarks in names unless the subject has the rights to use that name.

## **3.2 INITIAL IDENTITY VALIDATION**

Certificate applicants must communicate application requests for certificates to an authorized RA or LRA via a trustworthy process, but generally in person. An authorized RA, equipped with Registration Authority

hardware and software, may communicate authorizations to issue Certificates directly to the supporting CA electronically, provided all communication is secure. An LRA, who is not equipped with Registration Authority hardware and software, must transmit authorization requests to issue Certificates to the appropriate RA by secure means (i.e., digitally signed electronic means, via registered mail, or in person).

### **3.2.1 Method to Prove Possession of Private Key**

In the case where the CMA generates the key directly on the Subscriber's token, or in a key generator that benignly transfers the key to the Subscriber's token, then the end-entity is presumed to be in possession of the private key at the time of generation or transfer and proof of possession is not required. If the user is not in possession of the token during key generation, the CMA shall deliver the token to the Subscriber via an accountable method (see Section 6.1.2).

The CMA must obtain acknowledgment of receipt from the Subscriber of shipment or must revoke any certificates issued to that Subscriber. The CMA must deliver activation data for the private keys within the token or module to the Subscriber through a separate, secure communication unless the CMA delivers the token or module in person.

When the CMA delivers keyed hardware tokens to Subscribers, they must accomplish delivery in a way that ensures that they provide the correct tokens and activation data to the correct people. The CMA shall maintain a Subscriber token receipt validation record. When any mechanism that includes a shared secret (e.g., a password or PIN) is used, the mechanism shall ensure that the applicant and the CMA are the only recipients of this shared secret.

In those cases where the Subscriber causes the system to generate keys (e.g., remote emergency renewal), the Subscriber is required to prove possession of the private key that corresponds to the public key in the certificate request to the CMA.

### **3.2.2 Authentication of Organization Identity**

A Treasury PKI CA may issue certificates directly in the name of an organization rather than an individual for those functions and applications performed on behalf of the organization. The CMA must authenticate the identity of any organization that appears as a component of a subject name appearing in a certificate issued by the CA before processing the certificate application. Any organization requesting a certificate must have a PKI Sponsor to accept the obligations of the organization. This section pertains only to the authentication and naming of an organization as the subject in a certificate.

Requests for certificates in the name of an organization or group shall include the necessary identifying data of the Sponsor, the group or organization name, address, and documentation of the existence of the organization. This information will include but is not limited to the following:

- Organization identification and authorization
- Contact information to enable the CMA to communicate with the PKI Sponsor as required

The CMA shall verify this information, in addition to the authenticity and authorization of the requesting PKI Sponsor, authenticate the validity of any authorizations to be asserted in the certificate, and verify the

source and integrity of the data collected to an assurance level commensurate with the certificate assurance

level requested. The CPS will specify acceptable measures for authenticating both the organization and PKI Sponsor's identity and authorizations.

The CMA shall also include his or her own identity information and authentication declaration as outlined in Section 3.2.3. The PKI Sponsor shall present information sufficient for registration at the level of assurance requested, for both himself or herself and the non-human Entity (i.e., organization or group) requesting a certificate, and shall authenticate this information in person as prescribed in Section 3.2.3.

### **3.2.3 Authentication of Individual Identity**

PIV-I Hardware certificates shall only be issued to human subscribers.

#### ***3.2.3.1 Authentication of Human Subscribers***

For Subscribers (including all RAs/LRAs and PKI Sponsors of organizations, components, and minors or others not legally competent), the CMA shall ensure that the applicant's identity information is verified in accordance with this CP, the applicable CPS, and all applicable MOAs. The CMA must ensure that the applicant's identity information and public key are adequately bound. For each assurance level, the applicant must meet the minimum set of requirements identified in this section. A CMA may use mechanisms of equivalent or stronger assurance if documented in their CPS. The appropriate TPKI CA CPS will specify the acceptable procedures for authenticating a Subscriber's identity.

The CMA must record the process followed for each certificate. Process information shall depend upon the certificate's level of assurance and shall be addressed in the applicable CPS. In addition, the documentation and authentication requirements shall vary depending upon the level of assurance. At a minimum, process documentation and authentication requirements must include the following, depending on the level of assurance for issuance of each certificate:

- Identity of the applicant.
- Identity of the person performing the identification.
- A signed declaration by that person that he or she verified the identity of the applicant as required using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law; The signature on the declaration may be either a handwritten or digital signature using a certificate that is of equal or higher level of assurance as the credential being issued.
- If in-person or supervised remote<sup>1</sup> identity proofing is done, a unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s).
- The date of the verification; and
- A declaration of identity signed by the applicant using a handwritten signature or appropriate digital signature (see Practice Note) and performed in the presence of the person performing the

---

<sup>1</sup> The minimum requirements associated with supervised remote identity proofing are described in NIST SP 800-63A, Digital Identity Guidelines: Enrollment and Identity Proofing, Section 5.3.3.

## UNCLASSIFIED

identity authentication, using the format set forth at 28 U.S.C.1746 (declaration under penalty of perjury) or comparable procedure under local law.

Practice Note: In those cases in which the individual is in possession of a valid digital signature credential of equal or higher level of assurance or the signature certificate is generated immediately upon authentication of the applicant's identity, the applicant may sign the declaration of identity and certificate of acceptance using the digital credential. In the latter case, if the applicant fails to sign the declaration of identity then the certificate must be revoked.

**For All Levels:** As an alternative to presentation of identification credentials, the CMA may use other mechanisms of equivalent or greater assurance (such as comparison of biometric data to identities pre-verified to the standards of this policy, and obtained via authenticated interaction with secured databases).

**For Medium and High Assurance:** The CMA shall establish identity no more than 30 days before initial certificate issuance. Before enabling the applicant's certificate, the CMA shall personally verify the applicant's identity. Minors and others not legally competent to provide face-to-face registration information alone shall be accompanied by a person already certified by the PKI (i.e., a Sponsor), who will present information sufficient for registration at the level of the certificate being requested, for himself or herself, and the person accompanied. Persons not physically capable of providing face-to-face registration information shall be proxied by a person already certified by the PKI, who will present information sufficient for registration at the level of the certificate requested, for both himself or herself and the person unable to appear himself or herself.

An Entity certified by a State or Federal Entity as being authorized to confirm identities may perform in-person authentication on behalf of the RA/LRA. The certified Entity forwards the information collected from the applicant directly to the RA/LRA in a secure manner. Packages secured in a tamper-evident manner by the certified Entity satisfy this requirement; other secure methods are also acceptable. Such authentication does not relieve the RA/LRA of responsibility to verify the presented data.

**For PIV-I Certificates:** The following biometric data shall be collected during the identity proofing and registration process, and shall be formatted in accordance with [NIST SP 800-76] (see Appendix B):

- An electronic facial image used for printing the facial image on the card, as well as for performing visual authentication during card usage. A new facial image shall be collected each time a card is issued; and
- Two electronic fingerprints to be stored on the card for automated authentication during card usage.

The table below summarizes the identification requirements for each level of assurance.

**UNCLASSIFIED**

**TABLE 3-2, IDENTIFICATION REQUIREMENTS**

Assurance Level	Identification Requirements
Rudimentary	No identification requirement; applicant may apply and receive a certificate by providing his or her e-mail address.
Basic	<p>Identity may be established by in-person proofing before a RA/LRA; or by remotely verifying information provided by applicant through record checks with the applicable agency, credit bureaus, or similar databases to confirm that the information provided uniquely identifies an individual and that records are consistent with the application.</p> <p>Address confirmation:</p> <ul style="list-style-type: none"> <li>a) Issue credentials in a manner that confirms the address of record supplied by the applicant; or</li> <li>b) Issue credentials in a manner that confirms the ability of the applicant to receive telephone communications at a number associated with the applicant in records, while recording the applicant’s voice.</li> </ul>
Medium (all policies except PIV-I Hardware)	<p>Applicant shall establish identity by supervised remote or in-person proofing before the RA/LRA, Trusted Agent, or an Entity certified by a State or Federal Entity as being authorized to confirm identities; the proofing authority shall verify such information provided to ensure legitimacy. A trust relationship between the Trusted Agent and the applicant, based on an in-person antecedent, may suffice as meeting the in-person identity-proofing requirement. Credentials required are either one Federal Government-issued Picture ID, one REAL ID Act compliant picture ID, or two non-Federal Government IDs, one of which shall be a photo ID (e.g., Non-REAL ID Act compliant Drivers License). Any credentials presented must be unexpired.</p> <p>Clarification on the trust relationship between the Trusted Agent and the applicant, which is based on an in-person antecedent identity proofing event, can be found in the “FBCA Supplementary Antecedent, In-Person Definition” document.</p>
PIV-I Card Authentication, PIV-I Hardware	For PIV-I, credentials required are two identity source documents in original form. The identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 1115-0136, Employment Eligibility Verification. At least one document shall be a valid State or Federal Government-issued picture identification (ID). For PIV-I, the use of an in-person antecedent is not applicable.
High	Applicant shall establish identity by in-person or supervised remote appearance before the RA/LRA, or Trusted Agent; the proofing authority shall verify such information provided to ensure legitimacy. Credentials required are either one Federal Government- issued Picture ID, or two non-Federal Government IDs, one of which shall be a photo ID (e.g., Driver’s License).

### ***3.2.3.2 Authentication of Devices***

Some computing and communications devices (routers, firewalls, servers, etc.) and software applications will be named as certificate subjects. In such cases, the device must have a human sponsor. These certificates shall be issued only to devices under the issuing entity's control (i.e., require registration and validation that meets all issuing agency's requirements, as well as requiring re-validation prior to being re-issued). In the case a human sponsor is changed, the new sponsor shall review the status of each device under his/her sponsorship to ensure it is still authorized to receive certificates. The CPS shall describe procedures to ensure that certificate accountability is maintained. The sponsor is responsible for providing the following registration information:

- Equipment identification (e.g., serial number) or service name (e.g., DNS name) or unique software application name
- Equipment or software application public keys
- Equipment or software application authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the CA or RA to communicate with the sponsor when required

The registration information shall be verified to an assurance level commensurate with the certificate assurance level being requested. For certificates issued at the Common-Device and Common-Device-Hardware policies, registration information shall be verified commensurate with the Medium assurance level. The identity of the sponsor shall be authenticated by:

- Verification of digitally signed messages sent from the sponsor using a certificate issued at an equal or higher assurance level than the requested certificate under this policy; or
- In-person registration by the sponsor, with the identity of the sponsor confirmed in accordance with the requirements of section 3.2.3.1

### ***3.2.3.3 Authentication of Human Subscribers for Role-based Certificates***

There is a subset of human subscribers who will be issued role-based certificates. These certificates will identify a specific role on behalf of which the subscriber is authorized to act rather than the subscriber's name and are issued in the interest of supporting accepted business practices. The role-based certificate can be used in situations where non-repudiation is desired. Normally, it will be issued in addition to an individual subscriber certificate. A specific role may be identified in certificates issued to multiple subscribers, however, the key pair will be unique to each individual role-based certificate (i.e. there may be four individuals carrying a certificate issued in the role of "Chief Information Officer" however, each of the four individual certificates will carry unique keys and certificate identifiers). Roles for which role-based certificates may be issued are limited to those that uniquely identify a specific individual within an organization (e.g., Chief Information Officer is a unique individual whereas Program Analyst is not). Role-based certificates shall not be shared but shall be issued to individual subscribers and protected in the same manner as individual certificates. For pseudonymous certificates that identify subjects by their organizational roles, the CA shall validate that the individual either holds that role or has been delegated the authority to sign on behalf of the role.

## UNCLASSIFIED

The Treasury CAs shall record the information identified in Section 3.2.3.1 for a sponsor associated with the role before issuing a role-based certificate. The sponsor must hold an individual certificate in his/her own name issued by the same CA at the same or higher assurance level as the role-based certificate.

The procedures for issuing role-based tokens must comply with all other stipulations of this CP (e.g., key generation, private key protection, and Subscriber obligations).

Role-based certificates shall not assert the following certificate policies defined within this CP: PIV-I Hardware, PIV-I Card Authentication, PIV-I Content Signing. Additionally, role-based certificates shall not assert any of the policies used by Treasury from the FCPF (i.e., PIV Authentication, PIV Card Authentication, and PIV Content Signing).

### ***3.2.3.4 Authentication of Human Subscribers for Group Certificates***

Normally, a certificate shall be issued to a single Subscriber. For cases where there are several entities acting in one capacity, and where non-repudiation for transactions is not desired, a certificate may be issued that corresponds to a private key that is shared by multiple Subscribers. The Treasury PMA and/or RAs shall record the information identified in Section 3.2.3.1 for a sponsor from the Information Systems Security Office or equivalent before issuing a group certificate.

In addition to the authentication of the sponsor, the following procedures shall be performed for members of the group:

- The Information Systems Security Office or equivalent shall be responsible for ensuring control of the private key, including maintaining a list of Subscribers who have access to use of the private key, and accounting for which Subscriber had control of the key at what time.
- The subjectName DN must not imply that the subject is a single individual, e.g. by inclusion of a human name form.
- The list of those holding the shared private key must be provided to, and retained by, the applicable CA or its designated representative; and
- The procedures for issuing tokens for use in shared key applications must comply with all other stipulations of this CP (e.g., key generation, private key protection, and Subscriber obligations).

Group certificates shall not assert the following certificate policies defined within this CP: PIV-I Hardware, PIV-I Card Authentication, PIV-I Content Signing. Additionally, group certificates shall not assert any of the policies used by Treasury from the FCPF (i.e., PIV Authentication, PIV Card Authentication, and PIV Content Signing).

### **3.2.4 Non-verified Subscriber Information**

Except for the rudimentary assurance level, CMAs shall not include unverified information in certificates.

### **3.2.5 Validation of Authority**

For cross certification, the TPKE PMO shall validate the representative's authorization to act in the name of the organization and include such verification in the recommendation to the PMA.

Before issuing CA certificates or signature certificates that assert organizational authority, the CA shall validate the individual's authority to act in the name of the organization. For pseudonymous certificates that identify subjects by their organizational roles, the CA shall validate that the individual either holds that role or has been delegated the authority to sign on behalf of the role.

### **3.2.6 Criteria for Interoperation**

The PMA shall determine the criteria for cross certification with other Entities in accordance with Section 1.1.5 and the U.S. Government Public Key Infrastructure Cross Certification Methodology and Criteria (See <http://www.idmanagement.gov/federal-public-key-infrastructure>). Prior to approving a new cross certificate, the PMA verifies that the new cross certificate would not result in multiple paths to a CA already participating in the FPKI.

## **3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS**

### **3.3.1 Identification and Authentication for Routine Re-key**

Re-keying a certificate means that the CMA creates a new certificate that has the same characteristics and level as the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key) and a different serial number and possibly different validity period.

In the event that a TRCA re-key is required, the TRCA will seek to exchange new cross certificates with the FCPCA. For any subordinate TPKI CA that requires a re-key, the TRCA will issue its new certificate.

Before issuance, the subordinate CA shall identify itself through use of its current signature key or the initial registration process. If it has been more than three years since the subordinate CA identification, as required in Section 3.2, the TPKI subordinate CA shall re-establish identity through the initial registration process.

Subscribers must periodically obtain new keys and re-establish identity as defined in Section 3.2.

A TPKI CA may re-key Subscribers based on electronically authenticated Subscriber requests. Subscribers must stop using private keys before the public key expires. Confidentiality private keys do not have a lifetime so Subscribers may use these keys at any time to decrypt information.

For device certificates, identity may be established through the use of the device's current signature key or the signature key of the device's human sponsor, except that identity shall be established through the initial registration process at least once every nine years from the time of initial registration.

The following key lifetimes given are maximums. A program may always require shorter lifetimes. The following key lifetimes are for end entities, Section 5.6 provides TRCA key lifetimes:

**UNCLASSIFIED**

**TABLE 3-3, END ENTITIES CERTIFICATE LIFE TIMES**

<b>Assurance Level</b>	<b>Public Key Certificate Lifetimes</b>
Rudimentary	Signature & confidentiality keys re-key every three years
Basic	Signature & confidentiality keys re-key every three years
Medium (all policies) & PIV-I Card Authentication	Signature & confidentiality keys re-key every three years
High	Signature & confidentiality keys re-key every three years

Subscribers of TPKE CAs shall identify themselves for the purpose of re-keying as required below:

**TABLE 3-4, SUBSCRIBER ROUTINE RE-KEY IDENTITY REQUIREMENTS**

<b>Assurance Level</b>	<b>Routine Re-key Identity Requirements for Subscriber Signature and Encryption Certificates</b>
Rudimentary	Subscriber may establish identity through use of current signature key.
Basic	Subscriber may establish identity through use of current signature key, except that the Subscriber shall re-establish identity through initial registration process at least once every fifteen years from the time of initial registration.
Medium (all policies)	Subscriber may establish identity through use of current signature key, except that the Subscriber shall re-establish identity through initial registration process at least once every nine years from the time of initial registration, or as required by renewal of PIV Card.
PIV-I Card Authentication	For mediumDevice and mediumDeviceHardware certificates, identity may be established through the use of current signature key or using means commensurate with the strength of the certificate being requested, except that identity shall be established through initial registration process at least once every nine years from the time of initial registration.
High	Identity may be established through use of the current signature key certificate, except that identity shall be established through initial registration process at least once every nine years from the time of initial registration.

If Treasury implements the capability of associating authorizations with a certificate, including any conveyed or implied by the subject’s DN, the Subscriber and/or the Subscriber’s organization shall notify the appropriate CAs of the withdrawal of authorization. The CPS shall document the mechanisms used to notify the appropriate CAs of this action. In such instances, withdrawal of authorization may result in revocation of the old certificate and, if necessary, the issuance of a new certificate with a different public key and the appropriate associated authorizations.

### ***3.3.1.1 Certificate Renewal***

Renewing a certificate means creating a new certificate with the same name, key, and authorizations as the old one, but a new, extended validity period, and a new serial number. The TRCA shall not perform certificate renewal. Any certificate issued by a TRCA with a new serial number must contain a unique public key not previously certified. TPKE Subordinate CAs may renew certificates. A TPKE CA may renew a certificate if the public key has not reached the end of its validity, the associated private key has not been compromised, and the user name and attributes are still correct. The PKI CA need not revoke the old certificate, but may not re-key, renew, or update it further. See Section 4.6.

### ***3.3.1.1 Certificate Update***

Updating a certificate means creating a new certificate that has the same or a different key, a different serial number, and differs in one or more other fields, from the old certificate. TPKE subordinate CAs may or may not revoke the old certificate, but must not re-key, renew, or update it further. Except at Rudimentary assurance, if a Subscriber's common name is legally changed (e.g., due to marriage or divorce), then legal proof of the name change (i.e., the same requirements used to apply for a certificate) must be provided to the Designated Naming Authority to initiate the name change process in the directory structure. Once this change has taken place, the individual must appear before (or be validated by) an RA/LRA in order for an updated certificate having the new name to be issued.

When a TPKE CA updates its private signature key and thus generates a new public key, the TPKE CA shall notify all CAs, RAs, and Subscribers that rely on the CA's certificate of the change. For self-signed (i.e., TRCA) certificates, such certificates shall be conveyed to users in a secure fashion to preclude malicious substitution attacks.

### **3.3.2 Identification and Authentication for Re-key after Revocation**

For all levels of assurance, Subscribers requesting certificates after revocation, other than during a renewal or update action, must meet initial identity authentication and registration requirements, as indicated in Section 3.2 to obtain a new certificate (This applies to all certificates issued by both a TRCA and any TPKE subordinate CA).

## **3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST**

The CMA must authenticate revocation requests in accordance with Section 4.9.3. The CMA may authenticate requests to revoke a certificate using signatures generated with that certificate's associated private key, regardless of whether or not the private key has been compromised.

## **4. CERTIFICATE LIFE-CYCLE**

### **4.1 APPLICATION**

This policy identifies the minimum requirements and procedures that are necessary to support trust in the PKI, without imposing specific implementation requirements on CMAs or users, and specifies requirements for initial application for certificate issuance.

The TRCA shall issue end-entity certificates to trusted role PKI Program Team personnel where necessary for the internal operations of the PKI TRCA. The TRCA will not issue end-entity certificates for any other reasons.

#### **4.1.1 Submission of Certificate Application**

For the TRCA, the Treasury PMA shall submit the certificate application to the FPKIPA. For subordinate Treasury PKI CAs, subordinate and/or supported activities shall submit requests for subordinate PKI CA certificates to the Department of the Treasury PKI PMO using the contact information provided in Section

1.5.2. Subscriber applicants shall follow the procedures in Section 4.2 of this CP and the applicable CPS.

#### **4.1.2 Enrollment Process and Responsibilities**

Within the Department, only the TRCA shall apply for cross certification with the Federal PKI, using the procedures outlined in the FBCA CP, the U.S. Government Public Key Infrastructure Cross Certification Criteria and Methodology, and the MOA.

Only the TRCA shall cross certify with external CAs. A Certification Practices Statement, written to the format of the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 3647) shall accompany all such requests.

Entities applying for cross certification are responsible for providing accurate information on their certificate applications. Upon issuance by the TRCA, the CMA shall manually check each certificate issued to a CA to ensure the proper population of each field and extension with the correct information before delivering the certificate to the Entity.

All CMAs shall authenticate, and protect from modification, communications among PKI authorities supporting the certificate application and issuance process.

## **4.2 CERTIFICATE APPLICATION PROCESSING**

### **4.2.1 Performing Identification and Authentication Functions**

The CMA shall verify the accuracy of certificate application information, using procedures as specified in the applicable CPS, before issuing certificates.

For the TRCA, the Treasury PKI PMA shall validate acceptance of applicant identification and authentication.

## UNCLASSIFIED

For subordinate Treasury PKI CAs, the identification and authentication of the Subscriber must meet the requirements specified for Subscriber authentication as specified in Sections 3.2 and 3.3. If databases or other sources are used to confirm Subscriber attributes, then these sources and associated information sent to a CA shall require:

- When information is obtained through one or more information sources, an auditable chain of custody be in place.
- All data received or exchanged with the attribute information source be protected and securely exchanged in a confidential and tamper evident manner and protected from unauthorized access.

The applicant and the supporting CMA must perform the steps outlined in the applicable CPS when an applicant applies for a certificate. The CMA and Subscribers may perform these steps in any order that is convenient and that does not defeat security; however, they must complete all steps before certificate issuance.

CMAs shall authenticate and protect from modification all communications supporting the certificate application and issuance process using mechanisms commensurate with the protection requirements of the data. CMAs shall protect from unauthorized disclosure any electronic transmission of this data (i.e., encryption) commensurate with the protection requirements of the data.

### **4.2.2 Approval or Rejection of Certificate Applications**

The PMA shall require an initial compliance audit to ensure that the Treasury PKI CAs and

other Entity CAs are prepared to implement all aspects of the applicable CPS, before authorizing the Treasury PKI PMO to issue and manage certificates asserting Department of the Treasury certificate policies. Treasury PKI CAs shall only issue certificates asserting Department of the Treasury certificate policies upon receipt of written notification from the Treasury PMA authorizing them to do so.

Practice Note: key generation signing ceremony can serve as initial compliance audit.

The Treasury PKI PMO and RAs/LRAs may reject any Subscriber, group, or component application that is incomplete, or that contains information that they cannot verify as accurate in accordance with Section

4.2.1. The CMA may afford Subscribers and Sponsors the opportunity to complete and/or augment application information. Failure to do so will result in denial of PKI certificates; and the CMA shall submit a report via protected communications to the Treasury PKI PMO, outlining the circumstances and providing full identifying data about the applicant (i.e., Subscriber, organization, or device) and any Sponsor.

### **4.2.3 Time to Process Certificate Applications**

CMAs shall identify and authenticate Subscribers, organizations, components, and PKI Sponsors not more than 30 days prior to certificate issuance. Otherwise, the CMA must re-confirm the identity to ensure issuance of the certificates to the appropriate individual.

## **4.3 ISSUANCE**

### **4.3.1 CA Actions During Certificate Issuance**

It is the responsibility of the CMA to verify that the certificate information is correct and accurate. The CMA shall check all CA certificates to ensure that all fields and extensions are properly populated. The CMA shall not sign any certificate until the RA and/or LRA have completed all verifications and modifications, if any, to the CA's satisfaction, and the identification and authentication process set forth in the CP and appropriate CPS are complete.

If an RA or LRA denies a certificate request, then the CA shall not sign the requested certificate.

CMAs shall verify all authorization and other attribute information received from an applicant. In most cases, the RA or LRA is responsible for verifying applicant data, but if CAs accept applicant data directly from applicants, then the CA is responsible for verifying the applicant data. The CMA shall verify information regarding attributes via those offices or roles that have authority to assign the information or attribute. The applicable CPS describes these processes and relationships.

### **4.3.2 Notification to Subscriber of Certificate Issuance**

Where notification is not an integral component of the issuance process (e.g., when individual is present as the certificate is generated on their token), Treasury PKI CAs shall proactively notify Subscribers that certificates have been generated.

## **4.4 ACCEPTANCE**

Before a Subscriber can make effective use of the private key, the CMA shall convey their responsibilities to the Subscriber (or Sponsor in the case of group/organization or device certificates) as defined in Section 9.6.

For Rudimentary assurance, there is no stipulation. For all other assurance levels before a CA provides a Subscriber or Sponsor with the private key and allows its effective use, a CMA shall inform the Subscriber of the certificate's contents and responsibilities for its use and security; and require and document the Subscriber's acceptance of those obligations. The CPS outlines the specific steps for conveying responsibilities.

### **4.4.1 Conduct Constituting Certificate Acceptance**

Failure to object to the certificate or its contents constitutes acceptance of the certificate.

### **4.4.2 Publication of the Certificate by the CA**

As specified in 2.2.1, each Treasury PKI CA shall publish all CA certificates in the appropriate certificate repositories. Subscriber certificates may be published as well, except those that contain the FASC-N and/or UUID in the subject alternative name extension such as PIV Authentication certificates.

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

For the TRCA, the Treasury PKI PMA shall provide notification to all subordinate and cross certified entities, including the FPKIPA upon issuance of new CA or inter-organizational CA cross certificates. Such notification shall occur at least two weeks prior to issuance. The notification shall assert that the new CA cross-certification does not introduce multiple paths to a CA already participating in the FPKI. In addition, all new artifacts (CA certificates, CRLDP, AIA and/or SIA URLs, etc.) produced as a result of the event shall be provided to the FPKIPA within 24 hours following issuance.

### **4.5 KEY PAIR AND CERTIFICATE USAGE**

#### **4.5.1 Subscriber Private Key and Certificate Usage**

For High, Medium Hardware, Medium, and Basic Assurance, Subscribers shall protect their private keys from access by other parties. For Rudimentary assurance, this CP makes no stipulation. Section 1.4 outlines authorized and prohibited uses of PKI certificates.

The Treasury PKI CA shall specify restrictions in the intended scope of usage for a private key through certificate extensions, including the key usage and other extensions as needed, in the associated certificate.

#### **4.5.2 Relying Party Public key and Certificate Usage**

TRCA certificates issued to subordinate and cross certified CAs, shall specify restrictions on use through critical certificate extensions, including the key usage extensions. Basic constraints may also appear if set to critical in accordance with the FPKI-PROF. Treasury PKI CAs shall issue CRLs specifying the status of all unexpired certificates. Relying Parties should process and comply with this information whenever using Treasury PKI CA-issued certificates in a transaction.

### **4.6 CERTIFICATE RENEWAL**

Certificate renewal consists of issuing a new certificate with a new validity period and serial number while retaining all other information in the original certificate including the public key. Frequent renewal of certificates may assist in reducing the size of CRLs. The TRCA shall not perform certificate renewal for CA or Subscriber certificates.

Where permitted after certificate renewal, a Treasury PKI CA may or may not revoke the old certificate, but must not re-key, renew, or modify it further.

#### **4.6.1 Circumstance for Certificate Renewal**

Subordinate Treasury PKI CAs may renew Subscriber certificates if the public key has not reached the end of its validity period, the associated private key has not been compromised or expired, and the Subscriber name and attributes are unchanged. In addition, the validity period of the certificate must meet the requirements specified in Section 6.3.2. Treasury PKI CAs may also renew Subscriber certificates when the CA re-keys. The CMA may renew OCSP Responder certificates except that the aggregated lifetime of the public key shall not exceed the certificate lifetime specified in Section 6.3.2.

#### **4.6.2 Who May Request Renewal**

For subordinate Treasury PKI CAs that support renewal, the CA shall only accept renewal requests from certificate Subscribers, PKI Sponsors, or RAs. Additionally, a Treasury PKI CA may perform renewal of its Subscriber certificates without a corresponding request, such as when the CA re- keys.

#### **4.6.3 Processing Certificate Renewal Requests**

For Treasury PKI CAs that support renewal, the Treasury PKI PMO shall approve certificate renewal for reasons other than re-key of the PKI CA.

#### **4.6.4 Notification of New Certificate Issuance to Subscriber**

Subordinate Treasury PKI CAs shall proactively notify affected Subscribers of certificate renewal by any appropriate and secure means.

#### **4.6.5 Conduct Constituting Acceptance of a Renewal Certificate**

Failure to object to the certificate or its contents constitutes acceptance of the certificate.

#### **4.6.6 Publication of the Renewal Certificate by the CA**

Renewed certificates shall be published in accordance with Sections 2.2.1 and 4.4.2.

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

For subordinate Treasury PKI CAs, the responsible Operating Authority shall notify the Treasury PKI PMO.

### **4.7 CERTIFICATE RE-KEY**

Re-keying a certificate consists of creating new certificates with a different public key (and serial number) while retaining the remaining contents of the old certificate that describe the subject.

The new certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key. After certificate re-key, the CA may or may not revoke the old certificate, but must not re-key, renew, or modify it further. Re-key of a certificate does not require a change to the subjectName and does not violate the requirement for name uniqueness.

Subscribers of Entity CAs shall identify themselves for the purpose of re-keying as required in Section 3.3.

#### **4.7.1 Circumstance for Certificate Re-key**

The TRCA will issue new cross certificates to subordinate or cross certified CAs when a currently recognized subordinate or cross certified CA has generated a new key pair and a valid CPS exists between the TRCA and the subordinate or cross certified CAs.

#### **4.7.2 Who May Request Certification of a New Public Key**

The Treasury PKI PMA may request certification of a new public key for subordinate Treasury PKI CAs or cross certified Entity Principal CAs. For subordinate CAs that support re-key, the CA shall only accept such

requests from the subject of the certificate or PKI Sponsors. Additionally, CAs and RAs may initiate re-key of a Subscriber's certificates without a corresponding request.

#### **4.7.3 Processing Certificate Re-keying Requests**

For TRCA, before performing re-keys on cross certified or subordinate CAs, the Treasury PKI PMA shall identify and authenticate Principal CAs by performing the identification processes defined in Section 3.2 or 3.3. The validity period associated with the new certificate must not extend beyond the period of the MOA.

For subordinate CAs, see Sections 3.2 and 3.3.

#### **4.7.4 Notification of New Certificate Issuance to Subscriber**

The Treasury PKI PMO shall notify subordinate Treasury PKI CAs and cross certified Entity Principal CAs upon issuance of new certificates. Subordinate CAs shall proactively notify affected Subscribers of certificate renewal by any appropriate and secure means.

#### **4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate**

Failure to object to the certificate or its contents constitutes acceptance of the certificate.

#### **4.7.6 Publication of the Re-keyed Certificate by the CA**

Re-keyed certificates shall be published in accordance with Sections 2.2.1 and 4.4.2.

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

For the TRCA, the Treasury PKI PMA shall provide notification to all subordinate and cross certified entities, including the FPKIPA upon issuance of renewed inter-organizational CA cross certificates. For subordinate CAs, the responsible Operating Authority shall notify the Treasury PKI PMO.

### **4.8 MODIFICATION**

Certificate modification (a.k.a. update) consists of creating new certificates with subject information (e.g., a name or email address) that differs from the old certificate. For example, a subordinate Treasury PKI CA may perform certificate modification for a Subscriber whose characteristics have changed (e.g., has just received a medical degree). The new certificate may have the same or different subject public key.

After certificate modification, the Treasury PKI CA may or may not revoke the old certificate, but must not re-key, renew, or modify it further.

#### **4.8.1 Circumstance for Certificate Modification**

For the TRCA, the CA performs certificate modification if the subordinate Treasury PKI CA or cross certified Entity CA changes its name. For subordinate CAs and cross certified Entity CAs, the CA performs certificate modification if the subject changes their name or other identifying data included in the certificate.

The PKI PMO may also perform certificate modification at the request of a subordinate or cross certified CA for the following reasons:

- Modification of SIA extension
- Minor name changes (e.g., change XXCA to XXCA1) as part of key rollover procedures

#### **4.8.2 Who May Request Certificate Modification**

The Treasury PKI PMO or the subordinate CA (or cross certified Principal CA) PKI PMO may request certificate modification for subordinate Treasury PKI CAs (or cross certified Entity Principal CAs).

For subordinate Treasury PKI CAs that support modification, the CA shall only accept such requests from the subject of the certificate or PKI Sponsors. CAs and RAs may initiate modification of a Subscriber's certificates without a corresponding request in cases where the change is the result of a modification to the CA or the directory.

#### **4.8.3 Processing Certificate Modification Requests**

For the TRCA, the Treasury PKI PMO shall perform certificate modification at the direction of the PMA.

The validity period associated with the new certificate must not extend beyond the period of the MOA and the Security Officer must verify the information before the CA issues the modified certificate.

For subordinate Treasury PKI CAs, the Subscriber must provide proof of all Subscriber information changes to the RA/LRA or other designated agent; and the RA/LRA must verify the information before the CA issues the modified certificate.

#### **4.8.4 Notification of New Certificate Issuance to Subscriber**

The Treasury PKI PMA shall notify subordinate Treasury PKI CAs and cross certified Entity Principal CAs upon issuance of new CA certificates. Subordinate Treasury PKI CAs shall proactively notify affected Subscribers of certificate renewal or modification by any appropriate and secure means.

#### **4.8.5 Conduct Constituting Acceptance of Modified Certificate**

Failure to object to the certificate or its contents constitutes acceptance of the certificate.

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

Modified certificates shall be published in accordance with Sections 2.2.1 and 4.4.2.

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

For the TRCA, the Treasury PKI PMA shall provide notification to all subordinate and cross certified entities, including the FPKIPA upon issuance of modified inter-organizational CA cross certificates. For subordinate Treasury PKI CAs, the responsible Operating Authority shall notify the Treasury PKI PMO.

## 4.9 CERTIFICATE REVOCATION AND SUSPENSION

The CMA must authenticate all revocation requests. CMAs may authenticate requests to revoke a certificate using that certificate's associated private key, regardless of whether or not the private key has been compromised. For High, Medium Hardware, Medium, PIV-I Card Authentication, and Basic Assurance, all CAs shall publish CRLs.

For a planned revocation of CAs that issue certificates asserting OIDs from the Common CP, the PMA shall notify the FPKIPA at least two weeks prior to the revocation of the CA certificate.

### 4.9.1 Circumstances for Revocation

The CMA will revoke certificates issued by the TRCA under three circumstances:

- The first circumstance is when the PMA requests revocation of a TRCA-issued certificate. This will be the normal mechanism for revocation in cases where the PMA determines that a subordinate Treasury PKI CA or a cross certified Entity PKI does not meet the Treasury PKI CP requirements or certification of the Entity PKI is no longer in the best interests of the Department of the Treasury or the Federal Government.
- The second circumstance is when the Treasury PKI PMO receives an authenticated request from a previously designated official of the cross certified Entity responsible for the Principal CA.
- The third circumstance is when the Treasury PKI Program Team determines that an emergency has occurred that may affect the integrity of the certificates issued by a Treasury PKI CA. Under such circumstances, the following individuals may authorize immediate certificate revocation:
  - Treasury PMA
  - Treasury PKI PMO
  - Treasury PKI OA

The PMA shall review the emergency revocation as soon as practicable. The TRCA shall revoke, at a minimum, certificates for the reason of key compromise upon receipt of an authenticated request from a subordinate Treasury PKI CA or cross certified Entity. Whenever any of the above circumstances occur, the TRCA shall revoke the associated certificate and place it on the appropriate revocation list. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.

For the TRCA, subordinate Treasury PKI CAs, and cross certified Entity CAs, the CMA shall revoke a certificate when the binding between the subject and the subject's public key defined within a certificate, excluding DN changes, is no longer considered valid.

The CMA shall revoke a Subscriber certificate when the binding between the subject and the subject's public key defined within a certificate is no longer valid. Examples of circumstances that invalidate the binding are:

- The Subscriber can be shown to have violated the stipulations of its Subscriber obligations and/or agreement
- The private key is suspected of compromise

## UNCLASSIFIED

- The user, Affiliated Organization or other authorized party (as defined in the CPS) makes a formal authenticated request to the CMA asking to revoke his or her certificate
- Privileged attributes if implemented, asserted in the Subscriber's certificate are reduced

For Certificates that express an organizational affiliation, the CMA shall require that the organization must inform the CMA of any changes in the subscriber affiliation. If the affiliated organization no longer authorizes the affiliation of a Subscriber, the CMA shall revoke any certificates issued to that Subscriber containing the organizational affiliation. If an organization terminates its relationship with TPKE such that it no longer provides affiliation information, the CMA shall revoke all certificates affiliated with that organization.

Whenever any of the above circumstances occur, the CMA revokes the associated certificate and places it on the CRL. Once revoked, a certificate will remain on the CRL or ARL at least until the certificate expires.

### 4.9.2 Who Can Request Revocation

The PMA may direct revocation of a TRCA certificate, or certificate issued by the TRCA. Subordinate Treasury PKI CAs and cross certified Entity CAs shall accept, at a minimum, revocation requests from Subscribers. The CMA may support requests for certificate revocation from other parties as specified in

the appropriate CPS. A cross certified Entity Principal CA may always revoke the certificate it has issued to a TRCA without PMA action.

Within the TPKE, a CA may summarily revoke certificates within its domain. An RA may request the revocation of a Subscriber's certificate on behalf of any authorized party as specified in its CPS or Subscriber agreements. A Subscriber can request the revocation of his or her own certificate(s).

### 4.9.3 Procedure for Revocation Request

Upon receipt of a revocation request involving a TRCA-issued certificate, the Treasury PKI PMO shall authenticate the request and apprise the PMA. The PMA may take whatever measures it deems appropriate to verify the need for revocation. If the revocation request appears valid, the PMA shall direct the Treasury PKI PMO to revoke the certificate. The Treasury PKI PMO shall give prompt oral or electronic notification to previously designated officials in all subordinate Treasury PKI CAs and cross certified Entities having a Principal CA with which the TRCA interoperates.

Subordinate Treasury PKI CAs and cross certified Entity CAs that implement certificate revocation shall revoke certificates upon receipt of sufficient evidence of compromise or loss of the Subscriber's corresponding private key. A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and provide a means for the request to be authenticated (e.g., digitally, or manually signed). Where Subscribers use hardware tokens, revocation is optional if all the following conditions are met:

- The revocation request was not for key compromise;
- The hardware token does not permit the Subscriber to export the signature private key;
- The Subscriber surrendered the token to the PKI CMA;
- The token was zeroized or destroyed promptly upon surrender;

## UNCLASSIFIED

- The token has been protected from malicious use between surrender and zeroization or destruction.

For PIV-I and in all other cases not identified above, revocation of the certificates is mandatory. Even where all the above conditions have been met, revocation of the associated certificates is recommended.

If it is determined that a private key used to sign requests for the issuance of one or more new certificates may have been compromised, all certificates authorized since the date of actual or suspected compromise, the approval of which directly or indirectly chain back to that private key, shall be either revoked or shall be verified to be appropriately issued.

Upon receipt of a revocation request from the Subscriber or another authorized party, the CA shall authenticate the revocation request. At its discretion, the CA may take reasonable measures to verify the need for revocation. Revocation takes effect upon publication of status information.

For PKI implementations using hardware tokens, Subscribers shall surrender to their sponsoring organization (e.g., Affiliated Organization) or CMA (through any accountable mechanism) all cryptographic hardware tokens issued under the sponsoring organization whenever they become invalid or before leaving the organization. If the CA cannot obtain the hardware tokens when a Subscriber leaves an organization, then the CA, immediately upon notification, shall revoke all Subscribers' certificates associated with the unretrieved tokens with the reason specified as key compromise. If later recovered, the token shall be zeroized or destroyed promptly upon surrender and shall be protected from malicious use between surrender and being zeroized or destroyed. Destruction of hardware tokens shall be recorded by the CMA or delegate.

#### **4.9.4 Revocation Request Grace Period**

There is no grace period for revocation under this policy; the Subscribers and authorized parties must notify the CMA as soon as they identify the need to revoke a certificate. CAs will revoke certificates as quickly as practical upon receipt of a proper revocation request, and shall always revoke certificates within the time constraints described in Section 4.9.5. See also Section 9.6.3.

#### **4.9.5 Time within which CA must Process the Revocation Request**

The TRCA and subordinate CAs will revoke certificates as quickly as practical upon receipt of a proper revocation request. Revocation requests shall be processed before the next CRL is published, excepting those requests validated within two hours of CRL issuance. Revocation requests validated within two hours of CRL issuance shall be processed before the following CRL is published. A request is considered received when a Trusted Role authorized to revoke certificates, first accesses a valid request.

#### **4.9.6 Revocation Checking Requirements for Relying Parties**

This CP makes no stipulation. Use of revoked certificates could have damaging or catastrophic consequences. The Relying Party and/or System Accreditor should make any determinations on the matter of how often new revocation data should be obtained, considering the risk, responsibility, and consequences for using a certificate whose revocation status cannot be guaranteed.

#### 4.9.7 CRL Issuance Frequency

CRLs shall be issued periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information may be issued more frequently than the issuance frequency described below.

Certificate status information shall be published not later than the next scheduled update. This will facilitate the local caching of certificate status information for off-line or remote (laptop) operation.

Treasury CAs that only issue certificates to other CAs and that operate off-line must issue CRLs at least once every 31 days, and the nextUpdate time in the CRL may be no later than 32 days after issuance time (i.e., the thisUpdate time).

CAs that issue certificates to subscribers or operate on-line must issue CRLs at least once every 18 hours, and the nextUpdate time in the CRL may be no later than 180 hours after issuance time (i.e., the thisUpdate time).

Practice Note: Since many applications only check for a new CRL at nextUpdate, a longer nextUpdate time may result in applications continuing to rely on older CRLs even when a newer CRL is available. A longer nextUpdate time also increases the potential of a replay attack to validate a newly revoked certificate. Where the CRL nextUpdate exceeds 48 hours, Relying Parties should consider these risks and take appropriate measures to mitigate the risk. For high-risk, sensitive Relying Party applications suggested measures include configuring a preference for OCSP by applications, pre-fetching CRLs at least every 18 hours, and use of other compensating controls.

#### 4.9.8 Maximum Latency of CRLs

Treasury PKI CAs shall publish CRLs within four hours of generation. (See Section 4.9.7) The CAs shall publish each CRL no later than the time specified in the nextUpdate field of the previously issued CRL for same scope.

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

For all authentication levels except Rudimentary, Treasury shall support online certificate status checking via OCSP [RFC 2560]. Since the Department of the Treasury operates in some environments that cannot accommodate online communications, all Treasury PKI CAs shall be required to support CRLs.

Online Certificate Status Authority (OCSA) used for verifying certificates asserting Department of the Treasury certificate policies shall perform the following actions:

- Certificates indicated as being valid have a chain of valid certificates (valid as defined by X.509) linking back to the TRCA
- Each certificate in the certificate chain used to validate the certificate whose status is being requested is checked for revocation, such that the Relying Party need not check more than one OCSA to validate a Subscriber certificate
- The certificate status response makes clear which attributes, if any and if used, other than certificate subject name the OCSA authenticates

If an Entity CA supports on-line revocation/status checking, the latency of certificate status information distributed on-line by Entity CAs or their delegated status responders must meet or exceed the requirements for CRL issuance stated in Section 4.9.7.

**4.9.10 On-line Revocation Checking Requirements**

This CP makes no stipulation. Clients using online revocation checking need not obtain or process CRLs, at their own discretion.

**4.9.11 Other Forms of Revocation Advertisements Available**

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

- The alternative method must be described in the appropriate CPS.
- The alternative method must provide authentication and integrity services commensurate with the assurance level of the certificate being verified.
- Any alternate forms used to disseminate revocation information shall be implemented in a manner consistent with the security and latency requirements for the implementation of CRLs and online revocation and status checking in Sections 4.9.5, 4.9.7, 4.9.8, and 4.9.9.

**4.9.12 Special Requirements Related To Key Compromise**

In the event of a TRCA or Entity Principal CA private key compromise or loss, the cross certificates shall be revoked and a CRL shall be published at the earliest feasible time by the Treasury PKI PMO.

For subordinate Treasury PKI CAs, when a CA certificate is revoked or Subscriber certificate is revoked because of compromise, or suspected compromise, of a private key, a CRL must be issued as specified below:

**TABLE 4-1, EMERGENCY CRL ISSUANCE FREQUENCY**

<b>Assurance Level</b>	<b>Maximum Latency for Emergency CRL Issuance</b>
Rudimentary	No stipulation
Basic	18 hours after notification
Medium (all policies)	18 hours after notification
PIV-I Card Authentication	18 hours after notification
High	Six hours after notification

The CRL shall contain codes identifying the reason for revoking a certificate and/or specific key pair.

For CAs that only issue CA certificates and are operated in an off-line manner, the interval between routine CRL issuance shall not exceed 31 days. Such CAs must meet the requirements specified above for issuing

Emergency CRLs. (Note: Such CAs will also be required to notify the FPKI Management Authority upon Emergency CRL issuance.)

#### **4.9.13 Circumstances for Suspension**

For CA certificates, suspension is not permitted.

For end entity certificates with private keys residing on PIV cards, suspension is allowed. The Subscriber, Sponsor, or a Security Officer shall have reasonable knowledge of the whereabouts of the PIV card at the time of the suspension request and throughout the suspension period

For certificates with keys residing on any other token, suspension is not permitted.

#### **4.9.14 Who Can Request Suspension**

Sponsors and Security Officers are authorized to request suspension. Other parties, such as supervisors, security personnel, and adjudicators, may request suspension of certificates by providing a reason for the suspension request.

#### **4.9.15 Procedure for Suspension Request**

Any format that is used to request a suspension shall identify the certificate(s) to be suspended, explain the reason for suspension, include an estimated time for the resolution of the suspension, and allow the request to be authenticated (e.g., digitally or manually signed).

Once approved by the RA, the certificates on the PIV card shall be marked suspended and the serial numbers and other identifying information placed on a CRL, in addition to any other suspension or revocation advertisement mechanisms used.

A Security Officer or a Sponsor coming into possession of the PIV card during the suspension period they shall put the card into a locked state

The token shall be protected from malicious use between surrender and return to the Subscriber.

A Security Officer shall have reasonable knowledge of the whereabouts of the PIV card at the time of the suspension request and throughout the suspension period

#### **4.9.16 Limits on Suspension Period**

The certificate(s) may not be suspended for more than 9 months.

If the binding between the Subscriber and the certificate cannot be reestablished before the suspension period expires, then the certificate shall be revoked.

### **4.10 CERTIFICATE STATUS SERVICES**

Treasury PKI supports online certificate status checking via OCSP [RFC 2560] and stipulates policy about online certificate status checking in section 4.9.9 of this CP.

#### **4.10.1 Operational Characteristics**

No further stipulation.

#### **4.10.2 Service Availability**

No further stipulation.

#### **4.10.3 Optional Features**

No further stipulation.

### **4.11 END OF SUBSCRIPTION**

This CP makes no stipulation.

### **4.12 KEY ESCROW AND RECOVERY**

The TRCA shall not perform any encryption key recovery functions involving subordinate Treasury PKI CAs or cross certified Entity CAs and shall not store any information encrypted by the Treasury PKI CA public key that may require key recovery capabilities. However, when encryption key pairs need to be issued by the TRCA covering repository system access or for other purposes, the PMA shall publish applicable requirements for that purpose.

#### **4.12.1 Key Escrow and Recovery Policy and Practices**

All key management keys issued to human subscribers shall be escrowed and protected as specified in Federal PKI Key Recovery Policy (FED KRP). Other key management keys may be escrowed. Key escrow practices shall be identified in the issuing CA CPS, in a separate KRPS, or combination of the two.

Treasury PKI CA private keys are never escrowed.

Under no circumstances shall the Treasury PKI CA or any third party hold in trust a subscriber's private signature key.

#### **4.12.2 Session Key Encapsulation and Recovery Policy and Practices**

If session key recovery is implemented, it shall conform to the (FED KRP). The practices shall be identified in the issuing CA CPS, in a separate KRPS, or combination of the two.

## 5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

### 5.1 PHYSICAL CONTROLS

All Treasury PKI CA equipment, including CA cryptographic modules, shall be protected from unauthorized access at all times. The TRCA shall impose physical security requirements that provide similar levels of protection as those specified below. All the physical control requirements apply equally to the Treasury PKI Root, subordinate CAs, and any remote workstations used to administer the CAs except where specifically noted.

#### 5.1.1 Site Location and Construction

The location and construction of the facility housing Treasury PKI CA equipment, as well as sites housing remote workstations used to administer the CAs, shall be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards, high security locks, and intrusion sensors, shall provide robust protection against unauthorized access to CA equipment and records.

The location and construction of any facility housing CMA equipment and operations shall be in accordance with the Treasury Security Manual, TD P 15-71 (<https://my.treasury.gov/ApprovedDocuments/TD-P-15-71-Treasury-Security-Manual.pdf>).

#### 5.1.2 Physical Access

##### *5.1.2.1 Physical Access for CA Equipment*

The CMA staff and Treasury PKI facilities shall protect Treasury PKI CA equipment, to include remote workstations used to administer the CAs, from unauthorized access at all times. The security mechanisms shall be commensurate with the level of threat in the equipment environment. Since the Treasury PKI Treasury Root and subordinate CAs must plan to issue certificates at all levels of assurance, the Treasury PKI PMO shall operate and control all CAs on the presumption that each shall issue at least one High Assurance certificate.

The physical security requirements pertaining to Treasury PKI CAs shall include:

- 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.
- Ensure an access log is maintained and inspected periodically.
- Ensuring manual or electronic monitoring for unauthorized intrusion.

In addition to those requirements, the following requirements shall apply to Treasury PKI CAs that issue Medium, PIV Card Authentication, Medium Hardware, or High assurance certificates:

- Require two-person physical access control to both the cryptographic module and computer systems

Multiparty physical access control to CA equipment can be achieved by any combination of two or more trusted roles (see Section 5.2.2) as long as the tasks being conducted are segregated in accordance with the requirements and duties defined for each trusted role.

The CMAs shall inactivate removable CA cryptographic modules before storage. When not in use, the CMA staff shall place removable CMA cryptographic modules, removable media, and any activation information used to access or enable CMA cryptographic modules or CMA equipment, or paper containing sensitive plain-text information, in locked containers. Such containers shall be sufficient for housing equipment and information commensurate with the classification, sensitivity, or value of the information protected by the certificates issued by the CMA. CMA staff shall either memorize or record and store activation data in a manner commensurate with the security afforded the cryptographic module, and shall not store such data with the cryptographic module or removable hardware associated with remote workstations used to administer the CA.

A security check of the facility housing Treasury PKI CA equipment or remote workstations used to administer the CAs shall occur before leaving the facility unattended. At a minimum, the check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation
- Any security containers are properly secured
- Physical security systems are functioning properly
- The area is secured against unauthorized access

The Treasury PKI PMO shall explicitly designate a person or group of persons responsible for making such checks. When a group of persons is responsible, the Treasury PKI PMO shall maintain a log identifying the person performing a check in each instance. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated.

#### ***5.1.2.2 Physical Access for RA Equipment***

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

#### ***5.1.2.3 Physical Access for CSS Equipment***

Physical access control requirements for CSS equipment (if implemented) shall meet the Treasury PKI CA physical access requirements specified in Section 5.1.2.1.

#### ***5.1.2.4 Physical Access for CMS Equipment***

Physical access control requirements for CMS equipment containing a PIV-I Content Signing key shall meet the CA physical access requirements specified in 5.1.2.1.

**5.1.2.5 Physical Access for KED Equipment**

Physical access control requirements for KED equipment that store private keys shall meet the CA physical access requirements specified in 5.1.2.1 of this CP.

**5.1.2.6 Physical Access for DDS Equipment**

Physical access control requirements for DDS equipment that store or use private keys shall meet the CA physical access requirements specified in 5.1.2.1 of this CP.

**5.1.2.7 Physical Access for KRA and KRO Equipment**

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

**5.1.3 Power and Air Conditioning**

The facility housing CA equipment shall have power and air conditioning sufficient to create a reliable operating environment. Treasury PKI CAs shall have backup capability sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. In addition, the Treasury PKI CA directories (containing TPKI issued certificates and CRLs) shall have Uninterrupted Power sufficient for a minimum of six hours operation in the absence of commercial power. Treasury PKI CAs shall employ appropriate mechanisms to ensure availability of repositories as specified in Section 2.2.1.

**5.1.4 Water Exposures**

This policy makes no stipulation on prevention of exposure of CA equipment to water beyond that called for by Treasury Security Manual, TD P 15-71 and best business practice. The PKI PMO shall install CA equipment such that it is not in danger of exposure to water and ensure installation of moisture detectors in areas susceptible to flooding. The requirement excludes potential water damage from fire prevention and protection measures (e.g., sprinkler systems). Contingency plans for a CA that has sprinklers for fire control shall address recovery if the sprinklers malfunction, or cause water damage outside the fire area.

**5.1.5 Fire Prevention and Protection**

This policy makes no stipulation on fire prevention and protection of CA equipment beyond that called for by Treasury Security Manual, TD P 15-71, and best business practice. A description of the CMA's approach for recovery from a fire disaster shall be included in the Disaster Recovery Plan required by Section 5.7.

**5.1.6 Media Storage**

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

### **5.1.7 Waste Disposal**

CMAs shall remove or destroy normal office waste in accordance with local policy. The CMAs shall destroy media used to collect, transmit, or store sensitive information such that the information is unrecoverable before disposal. Sensitive waste material (i.e., documentation) shall be disposed of in a secure fashion (e.g., shredding or burning).

### **5.1.8 Off-Site Backup**

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

## **5.2 PROCEDURAL CONTROLS**

Unless stated otherwise, the requirements in this section apply equally to all Treasury PKI CAs.

### **5.2.1 Trusted Roles**

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible and above reproach or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust in the entire PKI.

There are two approaches to increase the likelihood of successfully carrying out these roles. The first approach is to ensure that the person filling the role is trustworthy and properly trained. The second is to distribute the functions of the role among several people, so that any malicious activity requires collusion. Chapter 1 describes the requirements regarding design and configuration of the technology to avoid mistakes and counter inappropriate behavior.

The requirements of this policy are defined in terms of the trusted roles detailed below. (Note: the information derives from the Certificate Issuing and Management Components (CIMC) Protection Profile.) Each CA shall maintain lists, including names, organizations, contact information, and copies of appointment memoranda of those who act in these trusted roles, and shall make them available during compliance audits. The CA will make this information a part of the permanent records of the CA. However, the CA shall not maintain personnel or investigative records requiring protection under the Privacy Act.

The following set of trusted roles apply to the CA, KED, and DDS. The roles may be maintained separately for each component, but the same role may be filled by the same individual(s) across multiple components:

- Administrator – authorized to install, configure, and maintain the CA, KED, or DDS; establish and maintain system accounts; configure profiles and audit parameters; and generate component keys.
- Officer – authorized to request or approve certificate issuances, certificate revocations, or key recoveries.
- Auditor – authorized to maintain audit logs.

- Operator – authorized to perform system backup and recovery.

Practice Note: If the KED is located within the CA, the same set of individuals may fill the CA roles and KED roles. If the DDS is located at a separate facility from the CA, and a separate department of the organization is responsible to maintain it, a separate set of individuals may be maintained as the DDS roles.

Section 5.2.4 identifies the roles required for each level of assurance. The following subsections provide a detailed description of the responsibilities for each role.

### **5.2.1.1 CA Trusted Roles**

The following roles apply to the CA:

#### **CA Administrator**

The CA Administrator role is responsible for the following:

- Installation, configuration, and maintenance of the CA
- Establishing and maintaining CA system accounts
- Configuring certificate profiles or templates and audit parameters
- Generating and backing up CA keys

Administrators do not issue certificates to Subscribers.

#### **Officer**

The Officer role includes the CA Security Officer and the Registration Authority roles, and is responsible for issuing certificates, that is:

- Registering new Subscribers and securely requesting the issuance of certificates
- Verifying the identity of Subscribers, validity of documentation, and accuracy of information included in certificates
- Approving and executing the issuance of certificates
- Requesting, approving and executing the revocation of certificates
- Receiving, controlling, and distributing Subscriber certificates on FIPS 140 Level 2 compliant hardware tokens (cryptographic modules containing the CA private key), as specified in this CP and the applicable Treasury CPS

The Officer also performs the administration and operation of the RA workstation.

#### **Auditor**

The Auditor role is responsible for the following:

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

## Operator

The Operator role is responsible for the routine operation of the CA equipment and operations such as system backups and recovery or changing recording media.

### **5.2.1.2 Key Recovery Trusted Roles**

Key recovery roles shall comply with the trusted role requirements in the Federal PKI Key Recovery Policy (FED KRP), but the roles are identified in this section to clarify how they fit amongst the other trusted roles. Key recovery roles include the Key Encryption Database (KED) roles, Data Decryption Server (DDS) roles, Key Recovery Agents (KRAs), and Key Recovery Officers (KROs).

The following roles apply to the Key Encryption Database (KED):

- KED Administrator
- KED Officer
- KED Auditor

The following roles apply to the Data Decryption Server (DDS):

- DDS Administrator
- DDS Officer
- DDS Auditor

### **5.2.2 Number of Persons Required per Task**

Only one person is required per task for CAs operating at the Rudimentary and Basic Levels of Assurance. Medium, Medium Hardware, and High assurance CAs shall enforce multi-person controls on the CA private signing key to prevent duplication or theft without collusion.

Two or more persons are required for the following tasks:

- CA key generation
- CA signing key activation
- CA private key backup

Where multiparty control for logical access is required, at least one of the participants shall be an Administrator. All participants must serve in a trusted role as defined in Section 5.2.1. Multiparty control for logical access shall not be achieved using personnel that serve in the Auditor Trusted Role.

Physical access to the CAs does not constitute a task as defined in this section. Therefore, multiparty physical access control may be achieved as specified in Section 5.1.2.1.

### **5.2.3 Identification and Authentication for Each Role**

At all assurance levels other than Rudimentary, an individual shall identify and authenticate him or herself before being permitted to perform any actions set forth above for that role or identity.

**5.2.4 Separation of Roles**

Role separation, when required as set forth below, may be enforced either by the CA equipment, procedurally, or both. Requirements for the separation of roles and limitations on use of procedural mechanisms to implement role separation for the TRCA and any subordinate CAs shall be as follows:

**TABLE 5-1, ROLE SEPARATION RULES**

Assurance Level	Separation Roles
Rudimentary	No stipulation
Basic	The CPS shall specifically designate individual CA personnel to the four roles defined in Section 5.2.1. In general, individuals may assume more than one role; however, no one individual shall assume both the Officer and Administrator roles. The Treasury PKI CAs may enforce this procedurally. No individual shall have more than one identity.
Medium (all policies)	The CPS shall specifically designate individual CA personnel to the four roles defined in Section 5.2.1. Individuals may only assume one of the Officer, Administrator, and Auditor roles, but generally, any individual may assume the Operator role. The CA and RA software and hardware shall identify and authenticate its users and shall ensure that no user identity can assume both an Administrator and an Officer role, assume both the Administrator and Auditor roles, and/or assume both the Auditor and Officer roles. No individual shall have more than one identity.
PIV-I Card Authentication	Individual personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Role separation duties follow the requirements for Medium assurance above.
High	The CPS shall specifically designate individual personnel to the four roles defined in Section 5.2.1. Individuals may assume only one of the Officer, Administrator, and Auditor roles. Generally, individuals designated as Officer or Administrator may also assume the Operator role. An auditor may not assume any other role.

Under no circumstances shall the incumbent of a CMA role perform its own external compliance auditor function. Only the CA Auditor may perform internal compliance auditor functions. The TRCA shall operate at the High Assurance level. The appropriate CPS designates the operating assurance level of individual subordinate CAs.

**5.3 PERSONNEL CONTROLS**

**5.3.1 Background, Qualifications, Experience, and Security Clearance Requirements**

The Treasury PKI PMO shall identify at least one individual or group responsible and accountable for the operation of each CA in the TPKI. For the TRCA, these are the Treasury PMO and the PKI PMO.

## UNCLASSIFIED

Selection for any CMA or other Treasury PKI trusted role is on the basis of loyalty, trustworthiness, and integrity. Trusted persons may be Department of the Treasury direct-hire personnel or contractors, but only U.S. citizens may fill trusted roles.

Only employees of the PKI Program Team shall fill Treasury PKI trusted roles, unless specifically appointed by the PKI PMO to satisfy operational requirements. Personnel appointed to any trusted roles shall meet the following requirements:

- Be employees of the Department of the Treasury, GS-5 (equivalent) or above, or equivalent contractor/vendor position of responsibility
- Have not been previously relieved of CMA related duties for reasons of negligence or non-performance of duties
- Have not been denied a security clearance, or had a security clearance revoked
- Have not been convicted of a felony offense
- Be appointed in writing by the Treasury PKI PMO

PKI Program Team personnel acting in the CA Administrator and CA Security Officer roles for the Treasury Root and subordinate CAs appointed by the PKI PMO, shall hold TOP SECRET security clearances.

### **5.3.2 Background Check Procedures**

PKI Program Team and other designated personnel acting in Trusted Roles shall undergo, at a minimum, background check procedures. Information obtained from such checks, performed solely to determine the suitability of a person to fill a PKI role, are not releasable except as required in Section 9.4.

Treasury PKI CA personnel shall pass, at a minimum, a background investigation covering the following areas:

- Employment
- Education
- Place of residence Law Enforcement
- References

The period of investigation must cover at least the last five years for each area, excepting the residence check, which must cover at least the last three years. Regardless of the date of award, the investigation shall verify the highest educational degree obtained.

A competent adjudication authority shall perform adjudication of the background investigation.

### **5.3.3 Training Requirements**

All personnel performing duties with respect to the operation of the Treasury PKI CAs shall receive comprehensive training in all operational duties they will perform, including disaster recovery and business continuity procedures.

The PKI Program Team must ensure appropriate training for all personnel involved in CMA operations. Training will address the following topics:

## UNCLASSIFIED

- Operation of the CMA software and hardware
- CA operational and security procedures and mechanisms
- Stipulations of this policy and local guidance
- All PKI software versions in use
- All PKI duties personnel shall perform
- Disaster recovery and business continuity procedures

The specific training required will depend on the equipment used and the personnel selected.

The PKI Program Team shall establish a training plan for a CMA installation. The PKI Program Team shall maintain documentation identifying all personnel who received training and the level of training completed. Where individuals demonstrated competence in lieu of training, the PKI Program Team shall maintain supporting documentation. CMA Training is the responsibility of the PKI Program Team, under the Treasury PKI PMO.

### **5.3.4 Retraining Frequency and Requirements**

Individuals responsible for PKI trusted roles shall be aware of changes in the Treasury PKI CA operation. Any significant change to CMA operations shall have a training (awareness) plan, and the PKI Program Team shall document execution of such plans. Examples of such changes are CA software or hardware upgrade, changes in automated security systems, and relocation of equipment. The PKI Program Team shall maintain documentation identifying all personnel who received training and the level of training completed.

### **5.3.5 Job Rotation Frequency and Sequence**

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

### **5.3.6 Sanctions for Unauthorized Actions**

A CMA shall report suspected security violations or compromises to the appropriate Security organization and the Treasury PKI PMO so that the proper authorities may take appropriate administrative and/or disciplinary actions against personnel who violate applicable policy.

The Treasury PKI PMO shall take appropriate actions where personnel have performed actions involving the Treasury PKI CAs or repositories not authorized in this CP, the appropriate CA CPS, or other procedures published by the Treasury PKI PMO.

### **5.3.7 Independent Contractor Requirements**

Contractor personnel employed to operate any part of the Treasury PKI CAs or perform functions pertaining to the Department's PKI infrastructure shall be subject to the same personnel requirements set forth in 5.3 of this CP. PKI subcontractors who provide services to the Department of the Treasury shall establish procedures to ensure that they perform in accordance with this policy.

### **5.3.8 Documentation Supplied to Personnel**

Personnel filling trusted roles shall receive documentation sufficient to define duties and procedures for each role. This documentation includes, but is not limited to this CP; relevant portions of the applicable

CPS, Contingency Plan, and KRPS; any relevant statutes, policies, and/or contracts; and any relevant programmatic documentation (e.g., CONOPS, Implementation Plan). Documentation may also include any handbooks, guidelines, or instructional manuals that have been or may be developed to ensure that personnel filling trusted roles are adequately trained.

## 5.4 AUDIT LOGGING PROCEDURES

Treasury PKI CAs shall generate audit log files for all events relating to the security of the CAs. Where possible, the CAs shall automatically collect security audit log data. For CAs operated in a virtual machine environment (VME), audit logs shall be generated for all applicable events on both the host and isolation kernel (i.e. hypervisor). Where this is not possible, the CMA shall use a logbook, paper form, or other physical mechanism. The CMA shall retain and make available during compliance audits all security audit logs, both electronic and non-electronic. The CMA shall maintain the security audit logs for each auditable event defined in this section in accordance with retention period for archive, Section 5.5.2.

### 5.4.1 Types of Events Recorded

A message from any source received by the TPKI requesting an action related to the operational state of a Treasury operated CA is an auditable event. The message must include message date and time, source, destination and contents. All security auditing capabilities of the CMA operating systems and applications required to meet this CP shall be enabled. As a result, most of the events identified in the table shall be automatically recorded. At a minimum, each audit record shall include the following (recorded either automatically or manually for each auditable event):

The type of event

The date and time the event occurred

A success or failure indicator when executing the applicable TPKI's signing process

A success or failure indicator when performing certificate revocation

Identity of the entity and/or operator (TPKI personnel) that caused the event

The table below lists detailed audit requirements according to the level of assurance. At a minimum, the CMA shall record (automatically or manually as appropriate) the events identified in the table for High Assurance.

**TABLE 5-2, AUDITABLE EVENT REQUIREMENTS**

<sup>1</sup> Represents scripted events that are only related to certification authorities. Therefore, the PMA/Internal Auditor is required to be present during these activities. These events are considered significant architectural CA or are designated as controlled events within the TPKI.

**UNCLASSIFIED**

<b>Auditable Events (Logged either electronically or manually)</b>	<b>Rudimentary</b>	<b>Basic</b>	<b>Medium (all policies) &amp; PIV-I Card Authentication</b>	<b>High</b>	<b>PMA Auditor or Script Required</b>
<b>SECURITY AUDIT</b>					
Any changes to the Audit parameters, e.g., audit frequency, type of event audited		X	X	X	
Any attempt to delete or modify the Audit logs		X	X	X	
Obtaining a third-party time-stamp		X	X	X	
<b>IDENTIFICATION AND AUTHENTICATION</b>					
Successful and unsuccessful attempts to assume a role		X	X	X	
The value of maximum authentication attempts is changed		X	X	X	
Maximum authentication attempts unsuccessful authentication attempts occur during user login		X	X	X	
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts		X	X	X	
An Administrator changes the type of authenticator, e.g., from password to biometrics		X	X	X	
<b>LOCAL DATA ENTRY</b>					
All security-relevant data that is entered in the system		X	X	X	X
<b>REMOTE DATA ENTRY</b>					
All security-relevant messages that are received by the system		X	X	X	
<b>DATA EXPORT AND OUTPUT</b>					
All successful and unsuccessful requests for confidential and security-relevant information		X	X	X	

**UNCLASSIFIED**

<b>Auditable Events (Logged either electronically or manually)</b>	<b>Rudimentary</b>	<b>Basic</b>	<b>Medium (all policies) &amp; PIV-I Card Authentication</b>	<b>High</b>	<b>PMA Auditor or Script Required</b>
<b>KEY GENERATION</b>					
Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)	X	X	X	X	X
<b>PRIVATE KEY LOAD AND STORAGE</b>					
The loading of Component private keys	X	X	X	X	X
All access to certificate subject private keys retained by the CA, RA, or LRA for key recovery purposes	X	X	X	X	
<b>TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE</b>					
All changes to the trusted public keys, including additions and deletions	X	X	X	X	
<b>SECRET KEY STORAGE</b>					
The manual entry of secret keys used for authentication			X	X	
<b>PRIVATE AND SECRET KEY EXPORT</b>					
The export of private and secret keys (keys used for a single session or message are excluded)	X	X	X	X	X
<b>CERTIFICATE REGISTRATION</b>					
All certificate requests and handling	X	X	X	X	X
<b>CERTIFICATE REVOCATION</b>					
All certificate revocation requests		X	X	X	X
<b>CERTIFICATE STATUS CHANGE APPROVAL</b>					
The approval or rejection of a certificate status change request		X	X	X	
<b>CA, RA or LRA CONFIGURATION</b>					
Any security-relevant changes to the configuration of the CA or the RA		X	X	X	X

**UNCLASSIFIED**

<b>Auditable Events (Logged either electronically or manually)</b>	<b>Rudimentary</b>	<b>Basic</b>	<b>Medium (all policies) &amp; PIV-I Card Authentication</b>	<b>High</b>	<b>PMA Auditor or Script Required</b>
<b>ACCOUNT ADMINISTRATION</b>					
Roles and users are added or deleted	X	X	X	X	
The access control privileges of a user account or a role are modified	X	X	X	X	
<b>CERTIFICATE PROFILE MANAGEMENT</b>					
All changes to the certificate profile	X	X	X	X	X
<b>CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT</b>					
All changes to the certificate revocation list profile		X	X	X	X
<b>MISCELLANEOUS</b>					
Appointment of an individual to a Trusted Role	X	X	X	X	X
Installation of the Operating System		X	X	X	X
Installation of CA, RA, or LRA Application		X	X	X	X
Installing hardware cryptographic modules			X	X	X
Removing hardware cryptographic modules			X	X	X
Destruction of cryptographic modules		X	X	X	X
System Startup		X	X	X	
Designation of personnel for multiparty control	X	X	X	X	X
Logon Attempts on CA, RA, or LRA Applications		X	X	X	
Receipt of Hardware / Software			X	X	
Attempts to set passwords		X	X	X	
Attempts to modify passwords		X	X	X	
Backing up CA, RA, or LRA internal database		X	X	X	

**UNCLASSIFIED**

<b>Auditable Events (Logged either electronically or manually)</b>	<b>Rudimentary</b>	<b>Basic</b>	<b>Medium (all policies) &amp; PIV-I Card Authentication</b>	<b>High</b>	<b>PMA Auditor or Script Required</b>
Restoring* CA, RA, LRA internal database (*Auditor present with scripts for COOP Drills and Designated CA Disaster Recovery Events only. Auditor not required for high availability or normal switch over of services between facilities.)		X	X	X	X
File manipulation (e.g., creation, renaming, moving)			X	X	
Posting of any material to a repository			X	X	
Access to CA, RA, or LRA internal database			X	X	
All certificate compromise notification requests		X	X	X	
Loading tokens with certificates			X	X	X
Shipment of Tokens			X	X	
Zeroize tokens		X	X	X	X
Rekey of the CA	X	X	X	X	X
<b>Configuration changes to the CA server RA, or LRA involving:</b>					
Hardware		X	X	X	X
Software		X	X	X	X
Operating System		X	X	X	X
Patches		X	X	X	X
Security Profiles			X	X	X
<b>PHYSICAL ACCESS / SITE SECURITY</b>					
Personnel Access to room housing CA			X	X	
Access to the CA server			X	X	
Known or suspected violations of physical security		X	X	X	

**UNCLASSIFIED**

<b>Auditable Events (Logged either electronically or manually)</b>	<b>Rudimentary</b>	<b>Basic</b>	<b>Medium (all policies) &amp; PIV-I Card Authentication</b>	<b>High</b>	<b>PMA Auditor or Script Required</b>
<b>ANOMALIES</b>					
Software Error conditions		X	X	X	
Software check integrity failures		X	X	X	
Receipt of improper messages			X	X	
Misrouted messages			X	X	
Network attacks (suspected or confirmed)		X	X	X	
Equipment failure	X	X	X	X	
Electrical power outages			X	X	
Uninterruptible Power Supply (UPS) failure			X	X	
Obvious and significant network service or access failures			X	X	
Violations of Certificate Policy	X	X	X	X	
Violations of Certification Practice Statement	X	X	X	X	
Resetting Operating System clock		X	X	X	

Similar events related to Subscribers, RAs, LRAs, or TAs activities do not require the PMA/Internal Auditor to be present. However, the logging of all other identified auditable events in the table above will still be enforced either by electronic or manual processes as per policy.

These events required configuration management and changes should be controlled through approved configuration change requests (CCRs). These scripts or CCRs will ensure that proper procedures are followed and to provide clear documentation of the changes made to the operational environment. These events are considered administrative in nature and therefore do not require the PMA/Internal Auditor to be present.

**5.4.2 Frequency of Processing Log**

Audit logs shall be reviewed by the Treasury PMA/Internal Auditor, in accordance with the table below and an audit alarm report shall be created by the PMA or Internal Auditor and submitted to the PMO for resolution. The Treasury PMO shall explain all significant events contained in the audit alarm report in an audit log summary. Such reviews involve verifying that the log has not been tampered with, and then inspecting a statistical set of all log entries, with a more thorough investigation of any alerts or irregularities

**UNCLASSIFIED**

contained within the logs. Actions taken because of these reviews shall be documented and reported to the PMA and any other appropriate authorities and entities in the same manner as outlined in Sections 8.5. The CMA shall implement procedures to transfer the security audit data to secure storage before overwriting or overflow of automated security audit log files.

**TABLE 5-3, AUDIT LOG REVIEW SCHEDULE**

<b>Assurance Level</b>	<b>Audit Log Review Schedule</b>
Rudimentary	Only required for cause.
Basic	Only required for cause or as mandated by Treasury security policy.
Medium (all policies) & PIV-I Card Authentication	At least once every two months ( $\leq 60$ days) Statistically significant set of security audit data generated by the CA since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity. This amount will be described in the CPS.
High	At least once every month ( $\leq 30$ days) Statistically significant set of security audit data generated by the CA since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity. This amount will be described in the CPS.

**5.4.3 Retention Period for Audit Log**

For Medium, Medium Hardware, and High Assurance CAs, the CMA shall retain audit logs on-site until reviewed, as well as retaining such logs in the manner described in Section 5.5. The CMA-equipment shall retain the security audit information it generates for at least two months, as outlined in Section 5.4.4, 5.4.5 and 5.4.6, until moved to an appropriate archive facility.

An entity other than the CMA (i.e., officials different from the individuals who, in combination, command the CA signature key) shall delete the security audit data from the CMA-equipment. The CPS shall identify the archival entity. The CMA shall retain security audit data as archive records in accordance with Section 5.5.

**5.4.4 Protection of Audit Log**

The security audit data shall not be open for reading or modification by any human, or by any automated process other than those that perform security audit processing. CMA must implement CA system configuration and procedures together to ensure that:

- Only personnel assigned to trusted roles have read access to the logs

- Only authorized people may modify, delete, or archive audit logs
- Audit logs are not modified
- The entity performing security audit data archive need not have “Modify” access, but procedures must be implemented to protect archived data from deletion or destruction before the end of the security audit data retention period. The archival entity shall move security audit data to a safe, secure storage location separate from the location where the data was generated

#### **5.4.5 Audit Log Backup Procedures**

The CMA shall backup audit logs and audit summaries at least monthly, and shall send a copy of the audit log off-site. The CMA shall protect the security audit data backup in accordance with the requirements of Section 5.4.4.

#### **5.4.6 Audit Collection System (Internal vs. External)**

The security audit process shall run independently, and the CMA shall not control it in any way. Treasury PKI CAs shall invoke security audit processes (automated and manual) at system or application startup, and cease only at system or application shutdown. In the event that the automated security audit system fails, the CMA shall cease all operations, except for revocation processing, until it can restore the security audit capability. Under these circumstances, the CMA shall employ mechanisms to preclude unauthorized CMA functions. The CPS shall describe these mechanisms.

#### **5.4.7 Notification to Event-Causing Subject**

This CP imposes no requirement to notify an individual, organization, device, or application that caused an auditable event. This policy neither requires nor prohibits real-time alerts.

#### **5.4.8 Vulnerability Assessments**

The CMA, system administrator, and other operating personnel shall routinely assess whether the CA system or its components have been attacked, breached, or for attempts to violate the integrity of the certificate management system, including the equipment, physical location, and personnel.

The security auditor shall review security audit data for events such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses. Security auditors shall check for continuity of the security audit data.

### **5.5 RECORDS ARCHIVE**

#### **5.5.1 Types of Events Archived**

CMA archive records shall collect and maintain enough detail to establish the proper operation of the Treasury PKI CAs, or the validity of any certificate (including revoked and/or expired) issued by the CA. At a minimum, the CMA shall archive following data, as well as all documentation required by compliance auditors:

**UNCLASSIFIED**

**TABLE 5-4, DATA ARCHIVAL REQUIREMENTS**

<b>Data To Be Archived</b>	<b>Rudimentary</b>	<b>Basic</b>	<b>Medium (all policies) &amp; PIV-I Card Authentication</b>	<b>High</b>
CA accreditation (if applicable)	X	X	X	X
Certificate Policy and Certification Practice Statement	X	X	X	X
Any contractual agreements (as appropriate) to which the CMA is bound, and other agreements concerning operations of the CA	X	X	X	X
System and equipment configuration	X	X	X	X
Modifications and updates to system, configuration, documentation (e.g., CPS), and contractual agreements	X	X	X	X
Certificate requests	X	X	X	X
Revocation requests		X	X	X
Documentation of receipt and acceptance of certificates		X	X	X
Documentation of receipt of tokens		X	X	X
All certificates issued or published	X	X	X	X
Record of CA Re-key and/or notification of cross certified CA Re-key in accordance with applicable MOAs	X	X	X	X
Signed records of every revocation (e.g., CRLs, CA application logs) providing validity status of any certificate at any time		X	X	X
All Audit Logs, and security audit data and reports	X	X	X	X
Other data or applications to verify archive contents		X	X	X
All CA operations communications and documentation to the PMA, PKI PA, other CMAs, and compliance auditors		X	X	X
Compliance Auditor reports		X	X	X

**5.5.2 Retention Period for Archive**

The minimum retention periods for archive data are identified below. Executive branch agencies must follow either the General Records Schedule established by the National Archives and Records Administration or an agency specific schedule as applicable. All other entities shall comply with their respective records retention policy in accordance with whatever law applies to that entity.

**TABLE 5-5, MINIMUM ARCHIVE RETENTION PERIOD**

Assurance Level	Audit Log Review Schedule
Rudimentary	7 Years 6 Months
Basic	7 Years 6 Months
Medium (all policies) & PIV-I Card Authentication	10 Years 6 months
High	20 Years 6 Months

**5.5.3 Protection of Archive**

Unauthorized users may not write to, modify, or delete the archive, but the CMA may move archived records to another medium as authorized by the PKI PMA. The CMA shall maintain a list of people authorized to modify or delete the archive from the system. Neither the CMA nor the archive site shall release the contents of the archive except: (1) in accordance with Department policy; or, (2) as required by law (See Sections 9.3 and 9.4). The CMA may release records of individual transactions upon request of any Subscribers involved in the transaction (i.e., originator or recipient), or their legally recognized agents.

Archive media shall be stored in a separate, safe, secure storage facility, not collocated with the Treasury PKI CAs. Before archiving, the CMA shall label archive records with the distinguished name, the date, and the classification of the information. Only authorized users may access the archive. The CMA will coordinate with Department Records Management Officials to ensure the scheduling and disposition approval by the NARA of all PKI archived records.

If the original media cannot retain the data for the required period, the PKI PMO shall define a mechanism to transfer the archived data to new media periodically. The Treasury PKI CAs shall provide archived data and the applications necessary to read the PKI archives to NARA or a Department of the Treasury approved archival facility for retention for at least the applicable retention period outlined above. Treasury CAs shall also maintain collateral PKI data records, which are those records documenting the operation of the PKI but not directly related to the system used to generate keys, certificates, and so forth in a similar manner.

Alternatively, a Treasury PKI CA may retain data using whatever procedures NARA has approved for that category of documents. The Treasury CMAs shall also maintain applications required to process the archive data for a period determined by the PKI PMA.

**5.5.4 Archive Backup Procedures**

No stipulation.

### **5.5.5 Requirements for Time-Stamping of Records**

Treasury PKI CA archive records shall be automatically time-stamped as they are created. The CMA is responsible for assuring that time stamps are consistent with an authoritative time standard. The CPS shall describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.

### **5.5.6 Archive Collection System (Internal or External)**

The Treasury PKI CA systems, or the CMA staff, may collect archive data in any expedient manner, provide the collection process does not modify or delete the archive records and protects the data as outlined in Section 5.5.3.

### **5.5.7 Procedures to Obtain and Verify Archive Information**

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

The CMA shall not release the contents of the archive except as determined by the PMA or as required by law. The CMA or archive site may release records of individual transactions upon request of any Subscribers involved in the transaction, or their legally recognized agents.

## **5.6 KEY CHANGEOVER**

CAs must not issue Subscriber certificates that extend beyond the expiration dates of their own certificates and public keys. Each Treasury PKI CA certificate validity period must extend one user certificate validity period past the last use of the CA private key. To minimize the risk from compromise of a CA's private signing key, the private signing key will change more frequently, and from that time on, certificate signing will use only the new key for certificate signing purposes. The older, but still valid, certificate will be available to verify old signatures until all of the user certificates signed under it have also expired. If the old private key signed CRLs that contain certificates also signed with that key, then the CA must retain and protect the old key.

For the TPKI, key changeover procedures will establish key rollover certificates where the new private key signs a certificate containing the old public key, and the old private key signs a certificate containing the new public key or must obtain a new CA certificate for the new public key from the issuers of their current certificates.

Practice Note: For example, a CA in a hierarchical PKI may obtain a new CA certificate from its superior CA rather than establish key rollover certificates.

After a CA performs a key changeover, the CA may continue to issue CRLs with the old key until all certificates signed with that key have expired. As an alternative, after all certificates signed with that old key have been revoked, the CA may issue a final long-term CRL using the old key, with a nextUpdate time past the validity period of all issued certificates. This final CRL shall be available for all relying parties until the validity period of all issued certificates has past. Once the last CRL has been issued, the old private signing key of the CA may be destroyed.

## 5.7 COMPROMISE AND DISASTER RECOVERY

### 5.7.1 Incident and Compromise Handling Procedures

The Treasury PMA shall notify the members of the Federal PKI Policy Authority, cross certified Entity CAs, and all subordinate CAs, if any, of the following cases occur:

- Suspected or detected compromise of TRCA systems.
- Physical or electronic attempts to penetrate TRCA systems.
- Denial of service attacks on TRCA components.
- Any incident preventing a TRCA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL.

This will allow other entities to protect their interests as Relying Parties.

The PKI Program Team shall reestablish operational capabilities as quickly as possible in accordance with procedures set forth in the TRCA CPS.

Subordinate CAs shall notify the PKI PMO and all other subordinate CAs shall provide similar notice. Entity CAs, cross certified to a TRCA, shall provide notice to the Treasury PKI PMO as required by the applicable MOA.

In the event of an incident as described above, the organization operating the CA shall notify the FPKIPA within 24 hours of incident discovery, along with preliminary remediation analysis. Within 10 business days of incident resolution, the organization operating the CA shall post a notice on its publicly available web page identifying the incident and provide notification to the FPKIPA. The public notice shall include the following:

1. CA components affected by the incident.
2. The CA's interpretation of the incident.
3. Who is impacted by the incident?
4. When the incident was discovered.
5. A complete list of all certificates that were either issued erroneously or not compliant with the CP/CPS because of the incident; and,
6. A statement that the incident has been fully remediated.

The notification provided directly to the FPKIPA shall also include detailed measures taken to remediate the incident.

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

When computing resources, software, and/or data are corrupted, the affected TRCA and subordinate CAs shall respond as follows:

- Before returning to operation, the CMA shall ensure that system integrity has been restored; and shall notify the PKI PMO and Treasury PMA.
- If the CA signature keys are not destroyed, CA operation shall be reestablished, giving priority to the ability to generate certificate status information within the CRL issuance schedule specified in Section 4.9.7.

## UNCLASSIFIED

- If the CA signature keys are destroyed, CA operation shall be reestablished as quickly as possible, giving priority to the generation of a new CA key pair.

In the event of an incident as described above, the organization operating the CA shall post a notice on its web page identifying the incident and provide notification to the FPKIPA. See Section 5.7.1 for contents of the notice.

### 5.7.3 Entity (CA) Procedures

In case of a CA key compromise or loss (such that compromise is possible even though uncertain) involving the TRCA:

- The Treasury PMA shall immediately notify the FPKIPA and all of its member entities so that those entities may issue CRLs revoking any cross certificates issued to the TRCA
- The TRCA CMA must remove the trusted self-signed certificate from each Relying Party application, and shall distribute a new one via secure out-of-band mechanisms. The TRCA will describe its approach to reacting to a TRCA key compromise in its CPS
- The PKI Program Team may generate a new TRCA key pair in accordance with procedures set forth in the TRCA CPS if so determined by the PMA
- The PKI Program Team may also issue new TRCA certificates to the FCPCA and all cross certified Entities in accordance with the TRCA CPS. If the CA distributes its key in a trusted certificate, the CMA shall distribute the new trusted certificate as specified in Section 6.1.4

In case of a CA key compromise or loss involving a subordinate CA:

- The TRCA shall revoke that CA's certificate, and publish the revocation information immediately in the most expedient manner
- The TRCA shall re-establish the subordinate CA installation as outlined herein
- The FPKIPA and all its member entities shall be notified
- If re-establishment is directed, the CMA shall generate a new CA key pair in accordance with procedures set forth in the appropriate CPS
- Upon re-establishment, the CMA shall issue new CA certificates to Entities also in accordance with the affected CA CPS

The PKI PMO shall also investigate and report to the Treasury PMA what caused the compromise or loss, and what measures have been taken to preclude recurrence and shall post a notice on its web page describing the compromise. See Section 5.7.1 for contents of the notice.

### 5.7.4 Business Continuity Capabilities after a Disaster

The PKI PMO shall maintain a Disaster Recovery Plan and shall operate a warm backup site, whose purpose is to ensure continuity of operations in the event of failure of the primary site. Treasury PKI CA operations shall be designed to restore full service within six hours of primary system failure. Treasury shall deploy the PKI CA directory system to provide 24 hour, 365 day per year availability. The PKI PMO shall implement features to provide high levels of directory reliability within the scope of its control.

## UNCLASSIFIED

In the case of a disaster damaging or rendering all CA equipment inoperative, the PKI Program Team shall re-establish affected CA operations as quickly as possible, giving priority to the ability to revoke certificates, regardless of type or user. For the TRCA, this will require secure out-of-band distribution of the new certificate as well as issuance of new cross certificates, subordinate CA certificates, and Subscriber certificates.

The PMA shall, at the earliest feasible time, securely advise the FPKIPA and all of its member entities in the event of a disaster where the TRCA installations are physically damaged and all copies of the TRCA' signature keys are destroyed. Relying Parties may decide of their own volition whether to continue to use certificates signed with the destroyed private key pending reestablishment of TRCA operation with new certificates.

In the case of a disaster causing physical damage to a subordinate CA installation and resulting in destruction of all copies of the CA signature key, the subordinate CA shall request revocation of its certificates. The PKI Program Team will then completely rebuild the CA installation by reestablishing the CA equipment, generating new private and public keys, be re-certified, and re- issue all cross certificates. Finally, all Subscriber certificates will be re-issued. Relying Parties may make a judgment to continue to use certificates signed with the destroyed private key to meet urgent operational requirements. In any event, the PMA shall securely notify all appropriate authorities (e.g., the FPKIPA, FPKI Management Authority, cross certified CAs, etc.) of the situation at the earliest feasible time in accordance with applicable MOAs and any other contractual agreements.

If a CA's signature keys are compromised, lost, or destroyed—such that compromise is possible even though uncertain—the PKI PMO shall cause an investigation to be conducted and report to the PMA concerning the cause of the compromise or loss and what measures have been taken to prevent recurrence. The PMA, in turn, will notify the appropriate authorities in accordance with applicable MOAs and any other contractual agreements.

### **5.8 CA & RA TERMINATION**

Treasury PKI CA termination will proceed in accordance with Section 9.10. In the event of termination of the TRCA operation, certificates signed by the TRCA shall be revoked and the Treasury PMA shall advise entities that have entered into MOAs with the Department's PKI that the TRCA operation has terminated so they may revoke certificates they have issued to the TRCA. Prior to TRCA termination, the PKI PMO shall provide all archived data to an archival facility. CMAs shall give cross certified entities as much advance notice as circumstances permit, and attempt to provide alternative sources of interoperation in the event the supporting TRCA is terminated.

In the case of subordinate CAs, if the termination is for convenience, contract expiration, re-organization, or other non-security related reason, and provisions have been made to continue compromise recovery, compliance and security audit, archive, and data recovery services, then neither the terminated CA's certificate, nor certificates signed by that CA, need to be revoked. For CAs ceasing operation, any issued certificates that have not expired, shall be revoked and a final long term CRL with a nextUpdate time past the validity period of all issued certificates shall be

## UNCLASSIFIED

generated. This final CRL shall be available for all relying parties until the validity period of all issued certificates has passed. Once the last CRL has been issued, the private signing key(s) of the CA to be terminated will be destroyed or taken offline, designated as “not in use”, and protected as stipulated in 5.1.2.1. If provisions for maintaining these services cannot be made, then the CA termination will be handled as a CA compromise in accordance with Section 4.9.12.

Before termination, the PMA shall securely notify all appropriate authorities (e.g., the FPKI Management Authority, cross certified CAs, etc.) of the situation at the earliest feasible time (at least two weeks if possible) in accordance with applicable MOAs and any other contractual agreements.

## 6. TECHNICAL SECURITY CONTROLS

### 6.1 KEY PAIR GENERATION AND INSTALLATION

#### 6.1.1 Key Pair Generation

This policy does not preclude any source of key generated in accordance with the stipulations of this policy and local security requirements. A private key must not appear outside of the module in which generated unless encrypted for local transmission or for processing or storage by a key recovery mechanism. Section 6.1.1.1 defines requirements for cryptographic modules used for key generation and storage.

##### 6.1.1.1 CA Key Pair Generation

The Treasury TRCA, subordinate CAs, and OCSPs shall generate cryptographic keying material used to sign certificates, CRLs or status information in FIPS 140 validated cryptographic modules. CA cryptographic modules shall meet or exceed FIPS 140 Security Level 3.

Multiparty control is required for CA key pair generation, as specified in Section 5.2.2.

The Treasury Root and subordinate CAs must document their key generation procedure in their respective CPSs, and generate auditable evidence that they followed the documented procedures. For all levels of assurance, the documentation of the procedure must provide enough detail to show the use of appropriate role separation. An independent third party shall validate the process either by witnessing or by examining the signed and documented procedures.

##### 6.1.1.2 Subscriber Key Pair Generation

The Subscriber, RA, or CA may perform Subscriber key pair generation. If the CA or RA generates Subscriber key pairs, the procedure must meet the requirements for key pair delivery specified in Section 6.1.2. All key generation shall be performed using a FIPS approved method.

At the High, PIV-I Card Authentication, and Medium Hardware assurance levels, the Subscriber, RA, or CA shall generate the Subscriber key pairs in hardware cryptographic modules validated to FIPS 140 Level 2 or above. For all other assurance levels, the Subscriber, RA, or CA shall use either validated software or hardware cryptographic modules for key generation.

For PIV-I Hardware certificates, to be used for digital signatures and/or authentication, and PIV-I Card Authentication certificates, subscriber key generation shall be performed on hardware tokens that meet the requirements of Appendix B.

##### 6.1.2 Private Key Delivery to Subscriber

If Subscribers generate their own key pairs, then there is no need to deliver private keys, and this section does not apply. If an Entity other than the Subscriber generates a private key, the CMA shall deliver the key to the Subscriber electronically or in a hardware token from which the private key cannot be extracted in unencrypted form. Any transmission of a private key over a network must use be encrypted.

## UNCLASSIFIED

In those cases where a Treasury PKI CA generates public/private key pairs on behalf of the Subscriber, the CA shall implement mechanisms to ensure that the public/private key pair is securely delivered to the proper Subscriber. The appropriate CPS describes this method.

For High and Medium Hardware assurance, a private key will be generated and must remain within the cryptographic boundary of the cryptographic module. If the CMA generates the key, then the CMA must also deliver the key module to the Subscriber. The Subscriber shall formally acknowledge receipt of the module. The CMA must maintain a record of the Subscriber acknowledgement of receipt of the token.

Under no circumstances shall any entity other than the Subscriber have knowledge of private signing keys. In the case of tokens (e.g., smart cards) the CA shall also implement procedures to ensure that the token is not activated by an unauthorized Entity. The CMA must send any key management private keys that are to be delivered over a network, encrypted and directly to the Subscriber's cryptographic module.

In all cases, the following requirements must be met:

- No one who generates a private signing key for a Subscriber shall retain any copy of the key after delivery of the private key to the Subscriber.
- The private key must be protected from activation, compromise, or modification during the delivery process.
- The Subscriber shall acknowledge receipt of the private key(s), regardless of the delivery means.
- Delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers.
- For hardware modules, accountability for the location and state of the module must be maintained until the Subscriber accepts possession of it.
- For electronic delivery of private keys, the key material shall be encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data shall be delivered using a separate secure means.
- For shared key applications, organizational identities, and network devices, see also Sections 3.2 and 3.3.

### **6.1.3 Public Key Delivery to Certificate Issuer**

For Treasury PKI CAs operating at the Basic, Medium, Medium Hardware, or High level of assurance, the following requirements apply:

- Where key pairs are generated by the Subscriber or RA, the public key and the Subscriber's identity must be delivered securely to the CA for certificate issuance.
- The delivery mechanism shall bind the Subscriber's verified identity to the public key. If cryptography is used to achieve this binding, it must be at least as strong as the CA keys used to sign the certificate.

For Rudimentary Assurance, this CP makes no stipulation.

The CMA shall deliver public keys to the certificate issuer in an authenticated manner set forth in the CPS.

#### 6.1.4 CA Public Key Delivery to Relying Parties

When a CA updates its signature key pair, the CA shall distribute the new public key in a secure fashion. The CA may distribute the new public key in a self-signed certificate, in a key rollover certificate, or in a new CA (e.g., cross) certificate obtained from the issuer(s) of the current CA certificate(s).

TRCA shall make their public keys available for creation and verification of certification trust paths, in the form of a self-signed public-key certificate. The CA shall deliver this self-signed certificate to Subscribers in a manner commensurate with the security offered by the public key in the certificate. CAs shall convey self-signed certificates to Relying Parties in a secure fashion to preclude substitution attacks. Such methods include, but are not limited to the following:

- Loading a self-signed certificate onto tokens delivered to Relying Parties via secure mechanisms
- Distribution of self-signed certificates through secure out-of-band mechanisms
- Comparison of certificate hashes against trusted certificate hashes made available via authenticated out-of-band sources (note that hashes posted in-band along with the certificate are not acceptable as an authentication mechanism)
- Downloading certificates from web sites secured with a currently valid certificate of equal or greater assurance level than the certificate downloaded

The CA shall sign the key rollover certificates with the CA's current private key, so secure distribution is not required.

#### 6.1.5 Key Sizes

This CP requires the use of RSA PKCS#1, RSA-PSS, or ECDSA signatures; additional implementation restrictions on key sizes and hash algorithms are specified below. Certificates issued under this policy shall contain RSA or elliptic curve public keys. Future revisions of this CP may specify any FIPS-approved signature algorithms that are considered acceptable. If the Treasury PMO determines that the security of a particular algorithm may have been compromised, the TPKE shall revoke all certificates signed by or asserting the compromised algorithm.

The key size requirements set forth in this section apply to both the CA signing key pair and the subscriber key pair. Treasury Subscriber certificates issued for assurance levels Rudimentary through Medium, and that expire on or before December 31, 2010 shall use at least 1024 bit RSA, DSA or Diffie Hellman (DH) and Secure Hash Algorithm version 1 (SHA-1 or better) in accordance with FIPS 186. Subscriber certificates issued under id-fpki-common-policy will comply with COMMON CP.

For CAs that distribute self-signed certificates to Relying Parties, the CA's subject public keys in such certificates shall be at least 2048 bits for RSA, or at least 256 bits for ECDSA. 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.

CAs that generate certificates and CRLs under this policy shall use signature keys of at least 2048 bit RSA key or at least 256 bits for ECDSA. All certificates, except self-signed certificates, that expire after 12/31/2030 shall be signed with keys of at least 3072 bits for RSA or at least 256 bits for ECDSA.

## UNCLASSIFIED

CAs that generate certificates and CRLs under this policy shall use SHA-256, SHA-384, or SHA-512 hash algorithm when generating digital signatures.

Where implemented, CSSs shall sign responses using the same signature algorithm, key size, and hash algorithm used by the CA to sign CRLs.

End entity certificates issued under id-fpki-common-authentication, id-fpki-common-device, and id-fpki-common-deviceHardware will contain RSA public keys that are 2048 bits.

End-entity certificates shall contain public keys that are at least 2048 bits for RSA, DSA, or Diffie- Hellman, or 256 bits for elliptic curve algorithms. The following special conditions also apply:

- End-entity certificates that expire after 12/31/2030 shall contain public keys that are at least 3072 bits for RSA or DSA, or 256 bits for elliptic curve algorithms.

Use of SSL/TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum AES (128 bits) or equivalent for the symmetric key, and at least 2048 bit RSA or equivalent for the asymmetric keys issued under High assurance and on or after 12/31/2010 at least 2048 bit RSA or 256 bit elliptic curve keys will be utilized by the protocol for all assurance levels. Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum AES (128 bits) or equivalent for the symmetric key, and at least 3072 bit RSA or equivalent for the asymmetric keys after 12/31/2030.

### **6.1.6 Public Key Parameters Generation and Quality Checking**

Treasury PKI CAs shall generate public key parameters for signature algorithms defined in the Digital Signature Standard (DSS) in accordance with FIPS 186. The CMA shall generate public key parameters in accordance with the standard that defines the cryptographic algorithm in which the parameters are used.

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

Treasury CAs shall certify public keys bound into certificates for use in signing or encrypting, but not both, except as specified below. The key usage extension in the X.509 certificate determines the use of a specific key. With the exception of the self-signed TRCA certificate, all certificates must have a populated key usage extension as defined in the X.509 key usage extensions. The key usage extension in the X.509 certificate determines the use of a specific key. Subordinate CAs shall set at least two key usage bits: cRLSign and keyCertSign. Where the subject signs OCSP responses, the certificate may also set the digitalSignature and/or nonRepudiation bits.

Subscriber certificates shall assert key usages based on the intended application of the key pair. Subscriber certificates to be used for digital signatures (including authentication) shall set the digitalSignature and/or nonRepudiation bits. However, a public-key certificate with key usage set for digitalSignature and keyEncipherment shall not also set for nonRepudiation. Certificates issued only for Authentication shall only set the digitalSignature bit. Certificates to be used for key or data encryption shall set the keyEncipherment and/or dataEncipherment bits. Certificates used for key encryption shall set the keyAgreement bit if the algorithm is DH and shall set the keyEncipherment bit if the algorithm is RSA. This restriction does not prohibit use of protocols that provide authenticated connections using key management certificates.

Certificates to be used for key agreement shall set the keyAgreement bit. If a certificate is used for authentication of ephemeral keys, the Key Usage bit in the certificate must assert the digitalSignature bit and may or may not assert keyEncipherment and keyAgreement depending on the public key in the certificate.

For end entity certificates issued after 30 June 2019, the Extended Key Usage extension shall always be present and shall not contain anyExtendedKeyUsage {2.5.29.37.0}. Extended Key Usage OIDs shall be consistent with key usage bits asserted.

Rudimentary, Basic, and Medium Assurance Level certificates may include a single key for use with encryption and signature in support of legacy applications. Treasury PKI CAs shall generate and manage such dual-use certificates in accordance with their respective signature certificate requirements, except where otherwise noted in this CP. Such dual-use certificates shall never assert the non-repudiation key usage bit and shall not be used for authenticating data that will be verified on the basis of the dual-use certificate at a future time. Treasury CAs shall issue Subscribers at all levels of assurance two key pairs: one for key management and one for digital signature, except where operationally necessary (e.g., VPN and web site/application access control). This restriction does not prohibit use of protocols that provide authenticated connections using key management certificates.

## 6.2 PRIVATE KEY PROTECTION & CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

### 6.2.1 Cryptographic Module Standards and Controls

The relevant standard for cryptographic modules is FIPS 140, Security Requirements for Cryptographic Modules.

NIST shall validate cryptographic modules to the FIPS 140 level identified in this section. Additionally, the Department of the Treasury reserves the right to review technical documentation associated with any cryptographic modules under consideration for use by the Treasury PKI CAs.

The following table specifies the minimum level of FIPS evaluation a cryptographic module must complete for use in the Department of the Treasury PKI:

**TABLE 6-1, MINIMUM LEVEL OF FIPS EVALUATION**

Assurance Level	CA & CSS	Subscriber	RA
Rudimentary	Level 1 (Hardware or Software)		Level 1 (Hardware or Software)
Basic	Level 2 (Hardware)	Level 1 (Hardware or Software)	Level 1 (Hardware or Software)
Medium	Level 2 (Hardware)	Level 1 (Hardware or Software)	Level 2 (Hardware)

UNCLASSIFIED

Assurance Level	CA & CSS	Subscriber	RA
PIV-I Card Authentication	Level 2 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)
Medium Hardware	Level 2 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)
High	Level 3 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)

The TRCA require Level 3 cryptographic modules as defined by FIPS 140. The TRCA may use a higher level if available or desired. Subordinate CAs shall sign certificates using a cryptographic module that meets Level 3 or higher.

The Treasury CA requires that all Subscribers issued certificates under id-fpki-common-hardware, id-fpki-common-devicesHardware, id-fpki-common-authentication, or id-fpki- common-cardAuth use a FIPS Level 2 or higher validated hardware cryptographic module for all private key operations.

All cryptographic modules shall operate such that the private asymmetric cryptographic keys never output in plain text. No private key shall appear unencrypted outside the CA equipment. No one shall have access to a private signing key but the subject of the corresponding certificate.

On an annual basis, for each PCI configuration used (as defined by the FIPS 201 Evaluation Program), one populated, representative sample PIV-I Card shall be submitted to the FIPS 201 Evaluation Program for testing.

PIV/PIV-I Card stock that has been removed from the APL may continue to be issued for no more than one year after GSA approved replacement card stock is available. PIV cards issued using the deprecated card stock may continue to be used until the current subscriber certificates expire, unless otherwise notified by the FPKIPA/FPKI Management Authority.

When a collection of private keys for multiple Subscriber certificates are held in a single location there is a higher risk associated with compromise of that cryptographic module than that of a single Subscriber. Where a single key store holds private keys for multiple Subscribers, the cryptographic module shall be no less than FIPS 140 Level 2 Hardware. In addition, authentication to the Cryptographic Device in order to activate the private key associated with a given certificate shall require authentication commensurate with the assurance level of the certificate.

**6.2.2 Private Key Multi-Person Control**

Use of Treasury CA private signing keys shall require action by multiple persons as set forth in Section 5.2.2 of this CP. Use of subordinate CAs private signing keys shall require action by multiple persons at Medium, Medium Hardware, and High Assurance as set forth in Section 5.2.2 of this CP.

Access to Medium, PIV-I Card Authentication, Medium Hardware, and High CA cryptographic modules shall be under two- person control. CMAs shall also back up key management and signature keys in multiple cryptographic modules under two-person control and ensure the security audit records the CMA backup actions. Only a CA may reproduce private keys in multiple cryptographic modules on behalf of Subscribers; neither RAs nor Subscribers shall duplicate private keys. The CMA may backup Treasury CA signature keys

only under two-person control. The CMA shall maintain a list of names of the parties used for two-person control.

### **6.2.3 Private Key Escrow**

#### ***6.2.3.1 Escrow of TRCA and Subordinate CA Private Signature Key***

Under no circumstances shall TRCA or subordinate CA signature keys used to sign certificates or CRLs be escrowed.

#### ***6.2.3.2 Escrow of CA Encryption Keys***

TRCA shall not perform any encryption key recovery functions involving encryption keys issued to subordinate CAs. However, if encryption key pairs need to be issued by the TRCA covering repository system access or for other purposes, the Treasury PMA shall publish applicable requirements for that purpose.

Subordinate CAs may escrow any encryption keys whose certificates do not contain the digital Signature key usage bit for the purpose of data recovery. The applicable CA CPS shall describe this method.

If a device has a separate key management key certificate, the encryption private key may be escrowed.

#### ***6.2.3.3 Escrow of Subscriber Private Signature Keys***

Subscriber private signature keys shall not be escrowed.

If a device has a separate encryption key pair, the encryption private key may be escrowed.

#### ***6.2.3.4 Backup of CSS Private Key***

Subscriber private dual use keys shall not be escrowed. Subordinate CAs shall escrow any encryption keys issued to human subscribers and may escrow other encryption key whose certificates do not also contain the digital Signature key usage bit for the purpose of data recovery. Escrow and recovery shall conform to the requirements of the (FED KRP).

### **6.2.4 Private Key Backup**

#### ***6.2.4.1 Backup of TRCA and Subordinate CA Private Signature Keys***

The TRCA shall back up private signature keys under multi-person control, as specified in Section 5.2.2. Backup of subordinate CA private signature keys is required to facilitate disaster recovery. Where required by Section 5.2.2, subordinate CAs shall back up private signature keys under multi-person control.

The CMA shall create backups of the TRCA and subordinate CA private signature keys on separate cryptographic modules. The CMA shall create these keys under the same multi-person control as the original signature key. Such backups shall create only a single copy of the TRCA and subordinate CA signature key at the primary CA location. The CA shall store at least one copy of each TRCA and each subordinate CA private signature key at the off-site backup location. The CMA shall account for and protect all copies of CA private signature keys in the same manner as the original.

All backup copies of CA private signature keys shall reside solely on cryptographic modules of equal strength and validation level as the primary. These levels are detailed in section 6.2.1

#### **6.2.4.2 Backup of Subscriber Private Signature Key**

At the Medium Hardware and High assurance levels, Subscriber private signature keys shall not be backed-up, escrowed, or copied.

Backed up subscriber private signature keys must be held under the subscribers' control and shall not be stored in plaintext form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the subscriber's cryptographic module.

#### **6.2.4.3 Backup of Subscriber Key Management Private Key**

Subordinate CAs may backup Subscriber key management private keys.

Subordinate CAs must encrypt backed up Subscriber key management private keys using an algorithm of a strength consistent with the private key being stored; or stored in a cryptographic module validated at FIPS 140 Level 2.

#### **6.2.4.4 Backup of CSS Private Key**

Treasury CAs may backup CSS private keys. If backed up, the CMA shall account for and protect all copies in the same manner as the original.

#### **6.2.4.5 Backup of Device Private Keys**

Device private keys may be backed up or copied, but must be held under the control of the device's human sponsor or other authorized administrator. Backed up device private keys shall not be stored in plaintext form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the device's cryptographic module.

### **6.2.5 Private Key Archival**

Treasury CAs shall not escrow or archive private signature keys as outlined in Section 6.2.3. Subordinate CAs may escrow or archive private encryption keys (key management or key transport) as outlined in Section 6.2.3.

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

TRCA and subordinate CA private keys shall be generated by and remain within a cryptographic module. At no time shall the CA private key exist in plain text outside the cryptographic module. The CMA may backup CA private keys in accordance with Section 6.2.4.1.

Subscriber private keys must be generated by and remain within a cryptographic module. In the event that a CMA transports a private key from one cryptographic module to another, the private key must be encrypted during transport. Private keys must never exist in plain text form outside the cryptographic module boundary.

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

### **6.2.7 Private Key Storage on Cryptographic Module**

This CP makes no further stipulation beyond that specified in FIPS 140.

### **6.2.8 Method of Activating Private Keys**

For the private keys of the TRCA and subordinate CAs that operate at the Medium, Medium Hardware, or High level of assurance and PIV-I Content Signing keys, signing key activation requires multiparty control as specified in Section 5.2.2.

Subscribers must use pass-phrases, PINS, biometric data, or other mechanisms of equivalent authentication robustness to authenticate to the cryptographic module before activating any private key in the cryptographic module for certificates at all levels of assurance. Section 6.4.1 specifies activation data generation requirements. The CMA must distribute activation data in person, or by an accountable method to the Subscribers separately from the cryptographic modules that they activate. Subscribers must protect the entry of activation data from disclosure using protections described in section 6.4.2.

For certificates issued under PIV-I Card Authentication, id-fpki-common-devices and id-fpki-common-devicesHardware, the device may be configured to activate its private key without requiring its human sponsor or authorized administrator to authenticate to the cryptographic token, provided that appropriate physical and logical access controls are implemented for the device and its cryptographic token. The strength of the security controls shall be commensurate with the level of threat in the device's environment, and shall protect the device's hardware, software, and the cryptographic token and its activation data from compromise.

### **6.2.9 Method of Deactivating Private Keys**

The CMA shall remove TRCA and subordinate CA cryptographic modules and store them in a secure container when not in use, as specified in Section 5.1.2.

Subscribers shall not leave activated cryptographic modules unattended or otherwise open to unauthorized access. When not in active use, they must be deactivated, e.g. via a manual logout procedure, by removing the cryptographic module, or automatically after a period of inactivity as defined in the applicable CA CPS. Subscribers shall remove and secure (e.g., under their personal control or in an approved security container) cryptographic module when not in use.

### **6.2.10 Method of Destroying Private Keys**

Individuals in trusted roles shall destroy CA, RA, and status server (e.g., OCSP server) private signature keys when no longer needed. Subscriber private signature keys shall be destroyed when no longer needed, or when the certificates to which they correspond expire or are revoked. For software cryptographic modules, this can be overwriting the data using a Treasury-approved utility and procedures. For hardware cryptographic modules, this will likely be executing a "zeroize" command. Private key destruction should not require physical destruction of hardware.

PKI Sponsors shall request the assistance of the LRA, RA, or CMA with the overwriting of software cryptographic modules used by hardware components and applications. Individual Subscribers shall take hardware tokens to the LRA, RA, or CMA for zeroizing to prevent accidental destruction of Access Control System or other resident data kept on the Smart ID Card/PIV Card.

### **6.2.11 Cryptographic Module Rating**

See Section 6.2.1

## **6.3 OTHER ASPECTS OF KEY MANAGEMENT**

A single dual-use (digital signature and encryption) key pair is prohibited for Medium Hardware and High Assurance implementations, but may be issued on a case-by-case basis for Rudimentary, Basic, and Medium Assurance levels. Such dual-use key pairs shall be issued only in support of legacy applications as defined in Section 6.1.7. Human Subscribers shall typically have one key-pair for digital signature, and a separate key-pair for encryption. A Subscriber's digital signature key-pair shall never be escrowed, archived, or backed-up, to maintain technical non-repudiation of transactions. For business continuity reasons, the CA may escrow, archive, or back-up encryption key-pairs.

### **6.3.1 Public Key Archival**

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

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

Treasury CAs that distribute their self-signed certificates for use as trust anchors shall limit the use of its private keys to a maximum of 20 years; the self-signed certificates shall have a lifetime not to exceed 37 years. For all other CAs, the CA shall limit the use of its private keys to a maximum of six years for

Subscriber certificates and ten years for CRL signing and OCSP responder certificates. Code and content signers shall use their private keys for a maximum of three years; the lifetime of the associated public keys shall not exceed eight years. Subscriber signature private keys and certificates shall have a maximum lifetime of three years. Signatures generated with these keys may be validated after expiration of the certificate. Subscriber key management certificates shall have a maximum lifetime of 3 years; use of Subscriber key management private keys is unrestricted. All restrictions on private-key usage periods are enforced procedurally.

For subscriber public keys in certificates that assert the id-PIV-content-signing OID in the extended key usage extension refer to the COMMON CP for future detail.

PIV-I subscriber certificate expiration shall not be later than the expiration date of the PIV-I hardware token on which the certificates reside. For PIV-I, CSS certificates that provide revocation status have a maximum certificate validity period of 31 days.

The validity period of the Subscriber certificate must not exceed the routine re-key Identity Requirements as specified in Section 3.3.1 or Key Changeover Requirements as specified in Section 5.6, as well as the CPS.

## 6.4 ACTIVATION DATA

### 6.4.1 Activation Data Generation and Installation

The activation data used to unlock TRCA, subordinate CA or Subscriber private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data protected. If the activation data must be transmitted, it shall be via an appropriately protected channel, and separate in time and place from the associated cryptographic module. Where the TRCA or a subordinate CA uses passwords as activation data for the CA signing key, the CMA shall change the activation data upon CA re-key at a minimum.

The activation data used by Subscribers to unlock private keys shall have an appropriate level of strength for the keys or data protected. Subscribers shall use passphrases, PINS, biometric data, or other mechanisms of equivalent authentication robustness to protect access to use of a private key for certificates at all other levels of assurance.

### 6.4.2 Activation Data Protection

Subscribers shall protect data used to unlock private keys from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data shall be:

- Memorized,
- Biometric in nature, or
- Recorded and secured at the level of assurance associated with the activation of the cryptographic module, and shall not be stored with the cryptographic module.

The protection mechanism shall include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts as set forth in the respective CPS.

Subscribers must never share activation data for private keys associated with certificates asserting individual identities. PKI Sponsors shall restrict activation data for private keys associated with certificates asserting group, organizational, non-human component identities to those in the organization authorized to use the private keys.

If transmission of the activation data must occur, it shall be via a channel with appropriate protection, and distinct in time and place from the associated cryptographic module. As part of the delivery method, users will sign and return a delivery receipt. In addition, users will also receive (and acknowledge) a user advisory statement to help to understand responsibilities for use and control of the cryptographic module.

### 6.4.3 Other Aspects of Activation Data

For PIV-I, in the event activation data must be reset, a successful biometric 1:1 match of the applicant against the biometrics collected in Section 3.2.3.1 is required. This biometric 1:1 match must be conducted by a trusted agent of the issuer.

## 6.5 COMPUTER SECURITY CONTROLS

### 6.5.1 Specific Computer Security Technical Requirements

For all Treasury PKI CAs, the computer security functions listed below are required. These functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. CAs and ancillary parts shall include the following functionality:

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

For subordinate CAs, the computer security functions listed below are also required. These functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. Subordinate CAs and ancillary parts shall include the following functionality:

- Authenticate the identity of Subscribers before permitting access to the system or applications
- Manage privileges of Subscribers to limit Subscribers to their assigned roles
- Generate and archive audit records for all transactions (see Section 5.4)
- Enforce domain integrity boundaries for security critical processes
- Support recovery from key or system failure

For CSS operating under this policy, the computer security functions listed below are required:

- Authenticate the identity of users before permitting access to the system or applications
- Manage privileges of users to limit users to their assigned roles
- Enforce domain integrity boundaries for security critical processes and provide process isolation, operating system self-protection, and residual information protection
- Support recovery from key or system failure

For remote workstations used to administer the CAs, the computer security functions listed below are required:

- Authenticate the identity of users before permitting access to the system or applications.
- Manage privileges of users to limit users to their assigned roles.

- Generate and archive audit records for all transactions; (see section 5.4).
- Enforce domain integrity boundaries for security critical processes; and
- Support recovery from key or system failure.

All communications between any PKI trusted role and the CA shall be authenticated and protected from modification.

### **6.5.2 Computer Security Rating**

When evaluated platforms host CA equipment in support of computer security assurance requirements, then the system (hardware, software, and operating system) shall operate only in an evaluated and certified configuration, per the Department of the Treasury Office of Cyber Security. At a minimum, such platforms shall use the same version of the computer operating system as received the evaluation rating.

## **6.6 LIFE CYCLE TECHNICAL CONTROLS**

### **6.6.1 System Development Controls**

The System Development Controls for the TRCA and subordinate CAs at the Basic Assurance level and above are as follows:

- The CAs shall use software designed and developed under a formal, documented development methodology.
- The CA shall use hardware and software specifically developed in a controlled environment; and the CMA shall define and document the development process which shall include software verification and validation requirements. This requirement does not apply to commercial off-the-shelf (COTS) hardware or software.
- Where developers use open source software, the developer/vendor shall demonstrate that security requirements were achieved through software verification & validation and structured development/life-cycle management.
- The PKI Program Team shall procure hardware and software to operate the CA in a fashion to reduce the likelihood of tampering with any component (e.g., by ensuring the random selection of material at time of purchase).
- The PKI Program Team shall dedicate CA hardware and software, including the VME hypervisor, to performing one task: operation and management of the CA. There shall be no other applications, hardware devices, network connections, or component software installed that are not part of the CA operation.
- The PKI Program Team shall take proper care to prevent malicious software from being loaded onto the CA equipment. RA hardware and software shall be similarly limited and scanned for malicious code on first use and continuously thereafter.
- Hardware and software updates shall be purchased or developed in the same manner as original equipment, and shall be installed by trusted and trained personnel in a defined manner.

### **6.6.2 Security Management Controls**

The PKI Program Team shall document and control the configuration of all CA systems as well as any modifications and upgrades. There shall be a mechanism for detecting unauthorized modification to the CA software or configuration. The PKI Program Team shall use the Department's formal configuration management methodology, through the IT-CCB, for installation and ongoing maintenance of the Treasury PKI CA systems. The PKI PMO shall verify the CA software, when first loaded, as that supplied from the vendor, with no modifications, and the version intended for use. The operator shall verify the integrity of CA software at least weekly.

### **6.6.3 Life Cycle Security Controls**

This CP makes no stipulation.

## **6.7 NETWORK SECURITY CONTROLS**

The PKI CMAs shall employ network security controls to protect the TRCA, the TRCA certificate repositories, and Certificate Status Servers. The CMA shall assure that all CMA equipment is protected (e.g., network guard, firewall, and/or filtering router) against known network attacks. The Treasury PKI CA system administrator shall turn off all unused network ports and services on the CAs and ensure that similar measures are taken on all guards, routers, and firewalls. Any network software present on CMA equipment shall be necessary to the functioning of the CMA application.

Subordinate CAs, RAs, supporting directories, remote workstations used to administer the CAs, and certificate status servers shall employ the same network security controls required of the TRCA, appropriate to their configuration.

- The CA shall establish connection with a remote workstation used to administer the CA only after successful authentication of the remote workstation at a level of assurance commensurate with that of the CA.
- The Treasury Directory shall be connected to the Internet and provide continuous service (except, when necessary, for brief periods of maintenance or backup) as outlined in Section 2.2.1. Any boundary control devices used to protect the directory, or any CA local area network shall deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.
- All boundary control devices shall only have user accounts required to administer the boundary control protections. The TRCA CPS shall define the respective network protocols and mechanisms required for operation of the Directory.

The TRCA is operated off-line; CRLs and ARLs are posted manually to the directories.

## **6.8 TIME STAMPING**

Asserted times shall be accurate to within three minutes. The PKI Program Team may use electronic or manual procedures to maintain system time. Clock adjustments are auditable events, see Section 5.4.

## 7. CERTIFICATE, CARL/CRL, AND OCSP PROFILES FORMAT

### 7.1 CERTIFICATE PROFILE

#### 7.1.1 Version Numbers

This policy uses X.509 Version 3 certificates exclusively.

The TRCA and subordinate CAs shall issue X.509 v3 certificates.

#### 7.1.2 Certificate Extensions

For all CAs, use of standard certificate extensions shall comply with [RFC 5280]. Certificates issued by the TRCA shall comply with Federal Public Key Infrastructure X.509 Certificate and CRL Extensions Profile [FPKI-Prof]. Certificates issued by subordinate CAs operating at High, Medium Hardware, and/or Medium Assurance shall also comply with [FPKI-Prof]. PIV Authentication Certificates issued by a subordinate CA under this policy may conform to the X.509 Certificate and CRL Extensions Profile for the SSP Program [SSP-PROF] instead.

Entity CAs that issue PIV-I Certificates shall comply with X.509 Certificate and CRL Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards [PIV-I Profile].

Practice Note: For Entity CAs that issue PIV-I certificates, the associated PIV-I Content Signing certificates will also comply with [PIV-I Profile] and an extended key usage of id-fpki-pivi-content- signing.

Treasury CA certificates shall not include critical private extensions. Subscriber certificates issued by subordinate CAs may include critical private extensions so long as interoperability within the community of use is not impaired. For PIV Auth certificates, the [SSP-Prof] defines the rules for the inclusion, assignment of value, and processing of extensions.

#### 7.1.3 Algorithm Object Identifiers

Certificates issued under this policy shall use one of the following OIDs for identifying the signature algorithm:

1. id-dsa-with-sha1 { iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3 }
2. sha-1WithRSAEncryption { iso(1) member-body(2) us(840) rsadis(113549) pkcs-1(1) 5 }
3. sha256WithRSAEncryption { iso(1) member-body(2) us(840) rsadis(113549) pkcs(1) pkcs-1(1) 11 }
4. id-RSASSA-PSS { iso(1) member-body(2) us(840) rsadis(113549) pkcs(1) pkcs- 1(1) 10 }
5. ecdsa-with-SHA1 { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) 1 }
6. ecdsa-with-SH224 { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 1 }
7. ecdsa-with-SH256 { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2 }
8. ecdsa-with-SHA384 { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 }

## UNCLASSIFIED

9. `ecdsa-with-SHA512 { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 4 }`

PIV Authorities shall sign certificates containing keys generated for use with OID `id-dsa-with-sha-256`, and for keys generated for use with RSA with sha-256WithRSAEncryption.

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

1. `id-sha256 { joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1 }`
2. `id-sha512 { joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 3 }`

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

<code>id-dsa</code>	<code>{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1}</code>
<code>id-ecPublicKey</code>	<code>{iso(1) member-body(2) us(840) ansi-x9-62(10045) id-publicKeyType (2) 1}</code>
<code>RsaEncryption</code>	<code>{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}</code>
<code>Dhpublicnumber</code>	<code>{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}</code>

Where non-CA certificates issued on behalf of federal agencies contain an elliptic curve public key, the parameters shall be specified as one of the following named curves:

1. `ansip192r1 { iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 1 }`
2. `ansit163k1 { iso(1) identified-organization(3) certicom(132) curve(0) 1 }`
3. `ansit163r2 { iso(1) identified-organization(3) certicom(132) curve(0) 15 }`
4. `ansip224r1 { iso(1) identified-organization(3) certicom(132) curve(0) 33 }`
5. `ansit233k1 { iso(1) identified-organization(3) certicom(132) curve(0) 26 }`
6. `ansit233r1 { iso(1) identified-organization(3) certicom(132) curve(0) 27 }`
7. `ansip256r1 { iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7 }`
8. `ansit283k1 { iso(1) identified-organization(3) certicom(132) curve(0) 16 }`
9. `ansit283r1 { iso(1) identified-organization(3) certicom(132) curve(0) 17 }`
10. `ansip384r1 { iso(1) identified-organization(3) certicom(132) curve(0) 34 }`
11. `ansit409k1 { iso(1) identified-organization(3) certicom(132) curve(0) 36 }`
12. `ansit409r1 { iso(1) identified-organization(3) certicom(132) curve(0) 37 }`
13. `ansip521r1 { iso(1) identified-organization(3) certicom(132) curve(0) 35 }`
14. `ansit571k1 { iso(1) identified-organization(3) certicom(132) curve(0) 38 }`
15. `ansit571r1 { iso(1) identified-organization(3) certicom(132) curve(0) 39 }`

### 7.1.4 Name Forms

In general, the TPKI will use the X.500 Distinguished Name (DN) in subject and issuer fields of the base certificate throughout the Department of the Treasury. As set forth in Section 3.1.1, the CMA shall populate

the subject and issuer fields of the base certificate with an X.500 Distinguished Name. Distinguished names shall be composed of standard attribute types, such as those identified in [RFC5280].

#### **7.1.5 Name Constraints**

Medium, Medium Hardware, and High assurance CA certificates issued shall impose name constraints and path length constraints as required by FPKI PROF.

#### **7.1.6 Certificate Policy Object Identifier**

Certificates issued under this policy shall assert the OID appropriate to the level of assurance in which issued, as defined throughout this policy. Additionally, a certificate may assert the OID of all lesser assurance levels. Section 1.2 identifies assurance levels of specific OIDs.

#### **7.1.7 Usage of Policy Constraints Extension**

The CAs may assert policy constraints in CA certificates. When this extension appears, at least one of requireExplicitPolicy or inhibitPolicyMapping shall be present. When present, this extension should be marked as noncritical to support legacy applications that cannot process policyConstraints. For Subordinate CA certificates inhibitPolicyMappings, skip certs will be set to 0. For cross-certificates inhibitPolicyMappings, skip certs will be set to 1. When requireExplicitPolicy is included skip certs will be set to 0.

#### **7.1.8 Policy Qualifiers Syntax and Semantics**

Certificates issued under this policy shall not contain policy qualifiers.

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

Processing semantics for any critical certificate policy extensions issued to Subscribers shall conform to FPKI PROF.

#### **7.1.10 Key Usage Constraints for id-fpki-common-authentication**

The CAs may assert InhibitAnyPolicy in CA certificates. When present, this extension should be marked as noncritical to support legacy applications that cannot process InhibitAnyPolicy. Skip Certs shall be set to 0, since certificate policies are required in the Federal PKI.

## **7.2 CRL PROFILE**

### **7.2.1 Version Numbers**

CRLs issued under this policy shall assert Version 2 described in the X.509 standard ISO 9594-8. The CRL shall always populate the nextUpdate field.

### **7.2.2 CRL Entry Extensions**

Detailed CRL profiles covering the use of each extension are available in FPKI PROF. For the Treasury Root and subordinate CAs, CRL extensions shall conform to [FPKI-PROF].

### **7.3 OCSP PROFILE**

CSS operating under this policy shall sign responses using algorithms designated for CRL signing. CSS shall be able to process SHA-1 hashes when included in the CertID field and the keyHash in the responderID field.

#### **7.3.1 Version Numbers**

CSS operating under this policy shall use OCSP version 1.

#### **7.3.2 OCSP Extensions**

CSS operating under this policy shall not use critical OCSP extensions

## **8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS**

The PMA shall have a compliance audit mechanism in place to ensure implementation and enforcement of the requirements of this CP and the applicable CPSs for subordinate CAs.

This specification does not impose a requirement for any particular assessment methodology.

Treasury CAs are subject to an annual review by the FPKIPA to ensure their policies and operations remain consistent with the policy mappings in the certificate issued to the TRCA by the FCPCA.

### **8.1 FREQUENCY OF AUDIT OR ASSESSMENTS**

All CAs, CMSs, and RAs shall be subject to a periodic compliance audit which is no less frequent than once per year for High, Medium Hardware and Medium Assurance, and at least once every two years for Basic Assurance. There is no audit requirement for CAs, RAs and LRAs operating at the Rudimentary Assurance level. Where a status server is specified in certificates issued by a CA, the status server shall be subject to the same periodic compliance audit requirements as the corresponding CA.

As an alternative to a full annual compliance audit against the entire CPS, the compliance audit of CAs and RAs may be carried out in accordance with the requirements as specified in the Triennial Audit Guidance document located at <http://www.idmanagement.gov/fpkipa/>.

The Treasury PMA shall have the right to require periodic compliance audits or inspections of subordinate CA, RA, LRA operations to validate that the subordinate entities are operating in accordance with their respective CPS. Further, the Treasury PMO has the right to require periodic compliance audits of the CAs in the TPKE.

### **8.2 IDENTITY & QUALIFICATIONS OF ASSESSOR**

The auditors must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with this policy and the appropriate CPS, as well as those of the FBCA and COMMON CP. The compliance auditor must perform PKI or Information System compliance audits as a regular ongoing business activity.

In addition to the previous requirements, the auditor must be a certified information system auditor (CISA) or IT security specialist and PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

Self-assessments shall be performed by an assessor that satisfies the qualifications listed for an Auditor. The assessor may also hold an Auditor trusted role position within the TPKE.

### **8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY**

Either the compliance auditor shall be a private firm, that is independent from the Entity being audited (CAs and RAs), or it shall be sufficiently organizationally separated from that Entity to provide an unbiased,

independent evaluation. An example of the latter situation may be an Agency inspector general. The PMA shall determine whether a compliance auditor meets this requirement.

The PKI PMO shall identify and recommend such auditors to the PMA. The PMA shall, in turn, approve the selection.

#### **8.4 TOPICS COVERED BY ASSESSMENT**

The compliance audit of the TRCA shall verify that the PKI PMO is implementing all provisions of the CPS approved by the PMA consistent with this CP. The audit shall also verify that the PKI PMO is implementing the relevant provisions of the MOAs between the Department and the FPKIPA.

The purpose of a compliance audit shall be to verify that the TRCA and the CMAs have in place a system to assure the quality of the CMA services that it provides, and that it complies with all of the requirements of this policy and the CPS for that Entity. All aspects of the CMA operation as specified in its CPS shall be subject to compliance audit inspections. In addition, the compliance audit shall verify that the Treasury PKI is correctly implementing the provisions of the MOA with the FPKIPA. A full compliance audit for the TRCA or subordinate CAs covers all aspects within the scope identified above.

#### **8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY**

When the compliance auditor finds a discrepancy between a CA or CMA's operation and the stipulations of this CP, the applicable CPS, and all applicable MOAs, the following actions must occur:

- The compliance auditor shall document the discrepancy and provide a copy to the PKI PMO
- The compliance auditor shall promptly notify the parties identified in Section 8.6 of the discrepancy
- The PKI PMO will propose a remedy, including expected time for completion, to the Treasury PKI PMA.
- The PKI PMA shall determine what further notifications or actions are necessary to meet the requirements of this CP, the CPS, and any relevant MOAs, and then proceed to make such notifications and take such actions without delay. The Treasury PMA may require a special compliance audit to confirm the implementation and effectiveness of the remedy.

#### **8.6 COMMUNICATION OF RESULTS**

Following each annual compliance audit of the Treasury PKI and the CA components operated by the Treasury PKI for its SSP customer organizations, the Treasury PMA shall provide an Audit Compliance Report letter to the Federal PKI Policy Authority. The letter shall be prepared in accordance with the "FPKI Annual Review Requirements" document and will include an assertion from the Treasury PKI PMA that all PKI components have been audited - including any components that may be separately managed and operated." The report shall identify the versions of the CP and CPS used in the assessment. The PMA shall communicate the audit results and implementation of remedies to appropriate entities in accordance with established MOAs, MOUs, and contractual agreements. Additionally, where necessary, the compliance auditor and/or Treasury PKI authorities shall communicate the results as set forth in Section 8.5.

## **9. OTHER BUSINESS & LEGAL MATTERS**

### **9.1 FEES**

The Department currently funds the Treasury Root and subordinate CAs centrally; however, the PMO reserves the right to charge a fee to external Agencies and internal Bureaus in order to operate the Treasury PKI CAs. The CAs will use these fees only to fund operation of the Treasury PKI CAs and fielding of PKI hardware and software beyond normally anticipated requirements (e.g., additional and/or special purpose certificates), based on the recommendation of the PKI PMO and PKI PMA.

#### **9.1.1 Certificate Issuance/Renewal Fees**

This CP makes no further stipulation.

#### **9.1.2 Certificate Access Fees**

This CP makes no further stipulation.

#### **9.1.3 Revocation or Status Information Access Fee**

This CP makes no further stipulation.

#### **9.1.4 Fees for other Services**

This CP makes no further stipulation.

#### **9.1.5 Refund Policy**

This CP makes no further stipulation.

### **9.2 FINANCIAL RESPONSIBILITY**

This CP contains no limits on the use of certificates issued by subordinate CAs under this policy, vis-à-vis the protection of financial transactions or information. Entities (e.g., bureaus, offices, posts, missions, external activities), acting as Relying Parties, shall determine, within their purview, what financial limits if any they wish to impose for certificates used to consummate a transaction; and shall implement applications at an appropriate level of assurance to support those limitations. The PMA and PKI PMO and other elements within the Department of the Treasury assume no financial responsibility or liability for those decisions.

#### **9.2.1 Insurance Coverage**

This CP makes no further stipulation.

#### **9.2.2 Other Assets**

This CP makes no further stipulation.

#### **9.2.3 Insurance/Warranty Coverage for End-Entities**

This CP makes no further stipulation.

### **9.3 CONFIDENTIALITY OF BUSINESS INFORMATION**

Treasury PKI CA information not requiring protection shall be made publicly available. The MOA shall address access to Treasury PKI CA information by the Federal PKI Policy Authority. The respective organization or bureau shall determine public access to Department information, in accordance with Department policy and Federal law.

#### **9.3.1 Scope of Confidential Information**

A certificate shall only contain relevant information necessary to effect secure transactions with the certificate. For the purpose of proper administration of the certificates, a CMA may request non-certificate information for use in managing the certificates within an organization (e.g., identifying numbers, business or home addresses and telephone numbers). The CPS shall explicitly identify any such information.

The CMA shall handle all information stored locally on the CA equipment and not in the repository as sensitive and restrict access to those with an official need-to-know in order to perform their official duties. The MOA will address access to Department of the Treasury information by the FPKIPA.

#### **9.3.2 Information not within the Scope of Confidential Information**

This CP makes no further stipulation.

#### **9.3.3 Responsibility to Protect Confidential Information**

A CMA shall not disclose non-certificate information to any third party unless authorized by this policy, required by U.S. law, U.S. government rule or regulation, or order of a U.S. court of competent jurisdiction. The PMA must authenticate any request for release of information.

### **9.4 PRIVACY OF PERSONAL INFORMATION**

#### **9.4.1 Privacy Plan**

The PMO shall conduct a Privacy Impact Assessment. If deemed necessary, the PKI PMO shall have a Privacy Plan to protect personally identifying information from unauthorized disclosure. The Department of the Treasury Privacy Officer shall approve the PKI Privacy Plan.

#### **9.4.2 Information Treated as Private**

Treasury PKI CAs shall protect all Subscribers personally identifying information from unauthorized disclosure. The Treasury PKI CAs shall also protect personally identifying information for Entity personnel collected to support cross certification and MOA requirements from unauthorized disclosure. The CMA may release records of individual transactions upon request of any Subscriber (i.e., originator or recipient) involved in the transaction, or their legally recognized agents. The CMA shall not release the contents of archives maintained by CAs operating under this policy except as required by law.

#### **9.4.3 Information not Deemed Private**

Information included in Treasury PKI CA certificates is not subject to protections outlined in Section 9.4.2.

For CAs, certificates that contain either the UUID or FASC-N in the subject alternative name extension shall not be distributed via publicly accessible repositories (e.g., Lightweight Directory Access Protocol (LDAP), HTTP).

#### **9.4.4 Responsibility to Protect Private Information**

All CMAs shall protect personal information from unauthorized disclosure as mandated by the Privacy Act of 1974, as amended. Sensitive information must be stored securely, and may be released only in accordance with other stipulations in Section 9.4.

#### **9.4.5 Notice and Consent to Use Private Information**

The PKI PMO is not required to provide any notice or obtain the consent of the Subscriber or Entity personnel in order to release private information in accordance with the stipulations of Section 9.4.

#### **9.4.6 Disclosure Pursuant to Judicial/Administrative Process**

The PKI PMO shall not disclose private information to any third party unless authorized by PMA, this policy, required by law, government rule or regulation, or order of a court of competent jurisdiction. Any request for the release of information shall be verified for authorization and authority to act in that capacity; before any data is released to the requesting official, and the release of information shall be processed according to 41 CFR 105-60.605.

#### **9.4.7 Other Information Disclosure Circumstances**

This CP makes no further stipulation.

### **9.5 INTELLECTUAL PROPERTY RIGHTS**

The PKI PMO will not knowingly violate intellectual property rights held by others. The U.S. Department of the Treasury owns any public key certificates and private keys that it issues.

### **9.6 REPRESENTATIONS & WARRANTIES**

The obligations described herein pertain to the TRCA (and, by implication, the PMO), and to all other CAs within the Department, or which either interoperate with the TRCA or are in a trust chain up to a Principal CA that interoperates with the TRCA. The obligations applying to Principal or other CAs pertain to their activities as issuers of certificates. Further, the obligations focus on external Entity CA obligations affecting interoperability with the TRCA. Thus, where the obligations include, for example, a review or audit by some other body other than a Department of the Treasury activity, the purpose of that review pertains to interoperability using the TRCA, and whether the Entities comply with the MOA.

The following obligations pertain to the Department of the Treasury PMA and PKI PMO:

- Approve the CPS for each Treasury PKI CA that issues certificates under this policy.
- Review periodic compliance audits to ensure that Treasury PKI CAs are operating in compliance with their approved CPS.

## UNCLASSIFIED

- Review name space control procedures to ensure that distinguished names are uniquely assigned for all certificates issued under this policy.
- Revise this CP to maintain the level of assurance and operational practicality.
- Publicly distribute this CP to all subordinate and cross certified CAs, all CMAs, and all Subscribers (distribution may be accomplished by making this CP available on a web site).
- Coordinate modifications to this CP to ensure continued compliance by subordinate CAs operating under approved CPSs.
- Review periodic compliance audits to ensure that RAs and other components operated by subordinate CAs are following their approved CPSs.

### **9.6.1 CA Representations and Warranties**

TRCA certificates are issued and revoked at the sole discretion of the Treasury PMA. When the TRCA issue a cross certificate to a non-federal Entity, it does so for the convenience of the U.S. Government and the Department of the Treasury. Any review by the Treasury PMA of a non-federal Entity's Certificate Policy is for the use of the PMA in determining whether or not interoperability is possible, and if possible, to what extent the non-federal Entity's Certificate Policy maps to the Treasury PKI X.509 CP.

For PIV-I, Entity CAs shall maintain an agreement with Affiliated Organizations concerning the obligations pertaining to authorizing affiliation with Subscribers of PIV-I certificates.

Any CA that issues certificates that assert the policy defined in this document shall conform to the stipulations of this document as outlined in the appropriate CPSs.

### **9.6.2 Registration Authority Representations and Warranties**

An RA or LRA who performs registration functions as described in this policy shall conform to the stipulations of this policy, and comply with the appropriate CPS approved by the PMA and PMO for use with this policy. RAs or LRAs performing registration functions for any Treasury PKI CA mapped to the FBCA shall also comply with the requirements of the Treasury—FPKIPA MOA. An RA or LRA found to have acted in a manner inconsistent with these obligations is subject to loss of RA or LRA privilege, and potentially adverse administrative or disciplinary action.

This policy distributes PKI duties between the CAs, and RAs and duties may vary among implementations of this Certificate Policy. For example, the RAs may merely collect information for a CA, or it may build the certificate for a CA to sign. CAs are ultimately responsible for ensuring that they sign only certificates

generated and managed in accordance with this policy. A CA shall ensure that only those who understand the associated Certificate Policy requirements, and who agree to abide by them perform certificate generation, management, and revocation functions.

Security requirements imposed on the TRCA are likewise imposed on any subordinate CAs, RAs and LRAs to the extent that the CAs, RAs and LRAs are responsible for the information collected. The particular assurance level asserted by a CA defines the specific information collected. A CMA found to have acted in a manner inconsistent with these obligations is subject to action as described in Section 8.5.

## UNCLASSIFIED

All CMAs supporting this policy shall conform to the stipulations of this document, as outlined in the appropriate CPSs.

### 9.6.3 Subscriber Representations and Warranties

For Medium (all policies), Medium Hardware, PIV-I, and High Assurance levels, a Subscriber shall be required to sign a document containing the requirements the Subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate. For Basic Assurance level, the Subscriber shall be required to acknowledge his or her obligations respecting protection of the private key and use of the certificate before being issued the certificate. Subscriber documents must be digitally signed, wherever possible.

Subscribers of Entity CAs at Basic, Medium (all policies), PIV-I and High Assurance Levels shall agree to and are obligated to perform the following:

- Accurately represent themselves in all communications with the PKI authorities and other Subscribers
- Always protect their private keys, in accordance with this policy, as stipulated in their certificate acceptance agreements and local procedures
- Comply with the requirements of this CP and the appropriate CPS, as well as the applicable requirements of the Treasury/FPKIPA MOA
- Notify, in a timely manner, the CMA that issued their certificates upon suspicion of loss or compromise of their private keys. Such notification shall be made directly or indirectly through mechanisms consistent with the CA's CPS
- Abide by all the terms, conditions, and restrictions levied on the use of their private keys and certificates
- Use certificates provided by the Department of the Treasury PKI only for transactions related to Department of the Treasury business

PKI Sponsors (as described in Sections 3.2.2 and 3.2.3) assume the obligations of Subscribers for the certificates associated with their organizations and hardware components.

If the PKI Sponsor for a device is not physically located near the sponsored device, and/or does not have sufficient administrative privileges on the sponsored device to protect the device's private key and ensure that the device's certificate is only used for authorized purposes, the device sponsor may delegate these responsibilities to an authorized administrator for the device. The delegation shall be documented and signed by both the device sponsor and the authorized administrator for the device. Delegation does not relieve the device sponsor of his or her accountability for these responsibilities.

### 9.6.4 Relying Parties Representations and Warranties

This CP does not specify the steps that an external 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 Treasury PKI CAs merely provide the tools (i.e., certificates, CRLs, and OCSAs) needed to perform the trust path creation, validation, and CP mappings that the relying party may wish to employ in its determination.

### **9.6.5 Representations and Warranties of Other Participants**

All CAs that issue certificates under this policy are obligated to post all CA certificates and all CRLs in a directory that is publicly accessible through the Active Directory and/or Lightweight Directory Access Protocol. To promote consistent access to certificates and CRLs, the repository shall implement access controls to prevent modification or deletion of information.

Posted certificates and CRLs may be replicated in additional repositories for performance enhancement. The TRCA and other CAs operating in accordance with this CP may operate such repositories.

All repositories that support a CA in posting information as required by this policy are obligated to accomplish the following:

- Maintain availability as required by the certificate stipulations of this policy
- Provide access control mechanisms sufficient to protect repository information
- Provide a repository service that accepts communications using the Active Directory and/or LDAP

### **9.7 DISCLAIMERS OF WARRANTIES**

CAs operating under this policy may not disclaim any responsibilities described herein.

### **9.8 LIMITATIONS OF LIABILITY**

The U.S. Government shall not be liable to any party, except as determined pursuant to the Federal Tort Claims Act (FTCA), 28 U.S.C. 2671-2680, or as determined through a valid express written contract between the Government and another party.

### **9.9 INDEMNITIES**

This CP makes no further stipulation.

### **9.10 TERM AND TERMINATION**

#### **9.10.1 Term**

This CP becomes effective when approved by the Treasury PMA. This CP has no specified term.

#### **9.10.2 Termination**

Termination of this CP is at the discretion of the Treasury PMA.

#### **9.10.3 Effect of Termination and Survival**

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

audits; and other business and legal matters shall remain in effect through the expiration date of the last certificate issued and/or cessation of operations and closure of the Treasury PKI.

### **9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS**

The Treasury PMA shall establish appropriate procedures for communications with CAs cross certified with this CP via MOAs/MOUs as applicable. Any planned changes to the infrastructure that has the potential to affect the FPKI operational environment shall be communicated to the FPKIPA at least two weeks prior to implementation.

For communications with subordinate CAs and all other communications, this CP makes no further stipulation.

### **9.12 AMENDMENTS**

#### **9.12.1 Procedure for Amendment**

The Treasury PMA shall review this CP at least once every year, and shall communicate approved corrections, updates, or suggested changes to this CP to the FPKIPA and cross certified Entity Principal CAs. Such communication shall include a description of the change, a change justification, and contact information for the person requesting the change.

Non-Federal policy changes under consideration by the Treasury PMA/PMO shall be disseminated to interested parties. Interested parties may provide their comments to the Treasury PMA.

All Federal CP change proposals approved, at the Federal PKI Policy Authority level, will be adapted as approved into the current version of the Treasury CP by virtue of that voting process.

#### **9.12.2 Notification Mechanism and Period**

The Treasury PMA shall make this CP and any subsequent changes publicly available within 30 days of approval (See Section 2.2).

#### **9.12.3 Circumstances under which OID must be Changed**

The Treasury PKI CA will change certificate OIDs if the FPKI Policy Authority determines that a change in the CP reduces the level of assurance provided.

### **9.13 DISPUTE RESOLUTION PROVISIONS**

Any dispute arising with respect to this policy or certificates issued under this policy shall be resolved by the Parties. The PMA decides any disputes over the interpretation or applicability of the Department of the Treasury PKI CP.

## **9.14 GOVERNING LAW**

United States Federal law (statute, case law, or regulation) govern the construction, validity, performance, and effect of certificates issued under this CP for all purposes. Where an inter-governmental dispute occurs, resolution will be according to the terms of the MOA.

## **9.15 COMPLIANCE WITH APPLICABLE LAW**

All CAs shall comply with applicable law. See Section 9.14.

## **9.16 MISCELLANEOUS PROVISIONS**

### **9.16.1 Entire Agreement**

This CP makes no further stipulation.

### **9.16.2 Assignment**

This CP makes no further stipulation.

### **9.16.3 Severability**

If it is determined that one section of this policy is incorrect or invalid, the other sections shall remain in effect until the next policy update. Section 9.1.2 describes the requirements for updating this policy. Responsibilities, requirements, and privileges of this document merge into the newer edition upon release of that newer edition.

### **9.16.4 Enforcement (Attorney Fees/Waiver of Rights)**

This CP makes no further stipulation.

### **9.16.5 Force Majeure**

This CP makes no further stipulation.

## **9.17 OTHER PROVISIONS**

This CP makes no further stipulation.

## APPENDIX A      Use of Common Policy Framework OIDs in Federal Legacy PIV Cards

Treasury PKI is a Federal Legacy PKI that pre-dated the Federal PKI SSP program. As such it operates a CA whose policies are typically mapped to those of the FBCA in order to establish interoperability with the Federal community. However, FIPS 201 requires that certificates contained in a PIV Card use specific certificate policies from the FCPCA. In response the FPKI PA issued a policy memo authorizing the Federal Legacies to use the policy identifiers from the FCPCA when issuing PIV Cards provided that certain criteria specified in the memo are met. For convenience, the memorandum has been included below.



### MEMORANDUM FOR FEDERAL AGENCY LEGACY PKIs

**SUBJECT:**      Implementing HSPD-12 using Legacy PKI certificates

Section 5.4.4 of FIPS 201 states: "Departments and agencies whose PKIs have cross-certified with the Federal Bridge CA (FBCA) at Medium-HW, or High Assurance Level may continue to assert department or agency-specific policy Object Identifiers (OID). Certificates issued on or after January 1, 2008 shall assert the id-CommonHW or id-CommonAuth policy OIDs. (Departments and agencies may continue to assert department or agency-specific policy OIDs in addition to the id-CommonHW and id-CommonAuth policy OIDs in certificates issued after January 1, 2008.)"

In order to facilitate Federal Legacy PKI compliance with this requirement, the Common Policy has been modified to include provisions that exclusively pertain to the Federal Legacy PKIs. By adding language pertaining to naming conventions and off-line root CAs, the main obstacles to compliance with the Common Policy by Federal Legacy PKI agencies have been removed. This should enable the Federal Legacy PKI agencies to express Common Policy OIDs in the PIV Authentication Certificates, as is required to meet the requirements of FIPS 201 (additional certificates for signing and key management can continue to only assert agency OIDs). However, those agencies planning to take advantage of this new language must ensure that they implement their certificates in a manner consistent with other provisions in the Common Policy. A Federal Legacy PKI will be deemed to be issuing PIV Authentication certificates in conformance with the Common Policy if it issues those certificates in accordance with the requirements of a certificate policy that has been mapped to the FBCA CP at the Medium Hardware or High assurance level and in accordance with the following additional provisions that affect certificate issuance:

- Identity proofing requirements (FIPS 201 Section 2)
- 18 hour CRL requirement (FIPS 201 Section 5.4.3) and the requirement to populate the nextUpdate field in CRLs as specified in the Common Policy, section 4.9.7.
- OCSP Requirement (FIPS 201 Sections 5.3 and 5.4)
- Requirement to issue the certificates in conformance with Worksheet 9 of the *X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program [SSP-PROF]* (FIPS 201 Section 5.4.2.1).

## APPENDIX B PIV-Interoperable Smart Card Requirements

The intent of PIV-I is to enable issuers to issue cards that are technically interoperable with Federal PIV Card readers and applications, and that may be trusted for particular purposes through a decision of the relying Federal agency. Thus, reliance on PIV-I Cards requires compliance with technical specifications and specific trust elements. This appendix defines the specific requirements of a PIV-I Card.

The following requirements shall apply to PIV-I Cards:

- To ensure interoperability with Federal systems, PIV-I Cards shall use a smart card platform that is on GSA's FIPS 201 Evaluation Program Approved Product List (APL) and uses the PIV application identifier (AID).
- PIV-I Cards shall conform to [NIST SP 800-73].
- The mandatory X.509 Certificate for Authentication shall be issued under treasury-pivi-hardware policy OID.
- All certificates issued under treasury-pivi-hardware, treasury-pivi-contentSigning, and treasury-pivi-cardAuth shall conform to [PIV-I Profile].
- PIV-I Cards shall contain an asymmetric X.509 Certificate for Card Authentication that:
  - conforms to [PIV-I Profile];
  - conforms to [NIST SP 800-73]; and
  - is issued under the treasury-pivi-cardAuth policy.
- PIV-I Cards shall contain an electronic representation (as specified in SP 800-73 and SP 800-76) of the Cardholder Facial Image printed on the card.
- The X.509 Certificates for Digital Signature and Key Management described in [NIST SP 800-73] are optional for PIV-I Cards.
- Visual distinction of a PIV-I Card from that of a Federal PIV Card is required to ensure no suggestion of attempting to create a fraudulent Federal PIV Card. Examples of allowable visual distinction includes (but are not limited to):
  - Printing a phrase on the front of the card, such as "PIV-Interoperable" or some other phrase that makes it clear this is not a PIV
  - Printing the card horizontal rather than in portrait mode
  - Using a colored background

If any non-Federally issued PIV-I cards are issued under this policy, images or logos shall not be placed entirely within Zone 11, Agency Seal, as defined by [FIPS 201].

- The PIV-I Card physical topography shall include, at a minimum, the following items on the front of the card:
  - Cardholder facial image.
  - Cardholder full name.
  - Organizational Affiliation, if exists; otherwise the issuer of the card; and
  - Card expiration date.
- PIV-I Cards shall have an expiration date not to exceed 6 years of issuance.

## UNCLASSIFIED

- Expiration of the PIV-I Card shall not be later than expiration of PIV-I Content Signing certificate on the card.
- The digital signature certificate that is used to sign objects on the PIV-I Card (e.g., CHUID, Security Object) shall contain the treasury-pivi-contentSigning policy OID. The PIV-I Content Signing certificate shall conform to [PIV-I Profile]
- The PIV-I Content Signing certificate and corresponding private key shall be managed within a trusted Card Management System as defined by Appendix C.
- At issuance, the RA shall activate and release the PIV-I Card to the subscriber only after a successful 1:1 biometric match of the applicant against the biometrics collected in Section 3.2.3.1.
- PIV-I Cards may support card activation by the card management system to support card personalization and post-issuance card update. To activate the card for personalization or update, the card management system shall perform a challenge response protocol using cryptographic keys stored on the card in accordance with [SP800-73]. When cards are personalized, card management keys shall be set to be specific to each PIV-I Card. That is, each PIV-I Card shall contain a unique card management key. Card management keys shall meet the algorithm and key size requirements stated in Special Publication 800-78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification. [SP800-78]

## APPENDIX C PIV-I Card Management System Requirements

PIV-I Cards are issued and managed through information systems called Card Management Systems (CMSs). The complexity and use of these trusted systems may vary. Nevertheless, Entity CAs have a responsibility to ensure a certain level of security from the CMSs that manage the token on which their certificates reside, and to which they issue certificates for the purpose of signing PIV-I Cards. This appendix provides additional requirements to those found above that apply to CMSs that are trusted under this Certificate Policy.

The Card Management Master Key shall be maintained in a FIPS 140-2 Level 2 Cryptographic Module and conform to [NIST SP 800-78] requirements. Diversification operations shall also occur on the Hardware Security Module (HSM). Use of these keys requires PIV-I Hardware or commensurate. Activation of the Card Management Master Key shall require strong authentication of Trusted Roles. Card management shall be configured such that only the authorized CMS can manage issued cards.

The PIV-I identity proofing, registration and issuance process shall adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a PIV-I credential without the cooperation of another authorized person.

Individual personnel shall be specifically designated to the four Trusted Roles defined in Section 5.2.1. Trusted Role eligibility and Rules for separation of duties follow the requirements for Medium assurance in Section 5.

All personnel who perform duties with respect to the operation of the CMS shall receive comprehensive training. Any significant change to CMS operations shall have a training (awareness) plan, and the execution of such plan shall be documented.

Audit log files shall be generated for all events relating to the security of the CMS shall be treated the same as those generated by the CA (see Sections 5.4 and 5.5).

A formal configuration management methodology shall be used for installation and ongoing maintenance of the CMS. Any modifications and upgrades to the CMS shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the CMS.

The CMS shall have document incident handling procedures that are approved by the head of the organization responsible for operating the CMS. If the CMS is compromised, all certificates issued to the CMS shall be revoked, if applicable. The damage caused by the CMS compromise shall be assessed and all Subscriber certificates that may have been compromised shall be revoked, and Subscribers shall be notified of such revocation. The CMS shall be re-established.

All Trusted Roles who operate a CMS shall be allowed access only when authenticated using a method commensurate with PIV-I Hardware.

The computer security functions listed below are required for the CMS: authenticate the identity of users before permitting access to the system or applications; manage privileges of users to limit users to their assigned roles; generate and archive audit records for all transactions; (see Section 5.4) enforce domain integrity boundaries for security critical processes; and support recovery from key or system failure.

## APPENDIX D Summary of Available Policies

The table below provides a high-level, informational summary of the types of certificates that Treasury issues to Subscribers. This table is non-normative and does not alter or negate any other policy statement found within this document.

Certificate Policy / OID	Description	Identity Proofing
Rudimentary / treasury-level 1 {2 16 840 1 101 3 2 1 5 2}	This level provides the lowest degree of assurance concerning identity of the individual. This level is relevant to environments in which the risk of malicious activity is considered low. It is not suitable for transactions requiring authentication, and is generally insufficient for transactions requiring confidentiality, but may be used for the latter where certificates having higher levels of assurance are unavailable.	This level requires the lowest degree of identity proofing and in-person proofing is not required. There is no identification requirement and the applicant may apply and receive a certificate by providing his or her e-mail address
Basic - Individual / treasury-level 2 {2 16 840 1 101 3 2 1 5 3}	This level provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but which are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high.	For Basic – Individual, identity may be established by in-person proofing before a Registration Authority or Trusted Agent; or remotely verifying information provided by applicant including ID number and account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that personal information in records are consistent with the application and sufficient to identify a unique individual. Address confirmation: a) Issue credentials in a manner that confirms the address of record supplied by the applicant; or b) Issue credentials in a manner that confirms the ability of the applicant to receive telephone communications at a number associated with the applicant in records, while recording the applicant’s voice.
Medium S/W / treasury-level 7 {2 16 840 1 101 3 2 1 5 7}	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having moderate monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is moderate. It is similar to Medium H/W except that the private key can be kept in software-based security modules.	For Medium S/W level of assurance, the Identity shall be established by in-person proofing before the Registration Authority or the Trusted Agent; information provided shall be verified to ensure legitimacy. A trust relationship between the Trusted Agent and the applicant which is based on an in-person antecedent may suffice as meeting the in-person identity proofing requirement. Credentials required are one Federal Government-issued Picture I.D., one REAL ID Act compliant picture ID1, or two Non-Federal Government I.D.s, one of which shall be a photo I.D. (e.g., Non-REAL ID Act compliant Drivers License). Any credentials presented must be unexpired.

**UNCLASSIFIED**

Certificate Policy / OID	Description	Identity Proofing
		Clarification on the trust relationship between the Trusted Agent and the applicant, which is based on an in-person antecedent identity proofing event, can be found in the "FBCA Supplementary Antecedent, In-Person Definition" document.
Medium H/W / treasury-level 3 {2 16 840 1 101 3 2 1 5 4}	This level is relevant to environments where threats to data are high or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk. The private key must reside on a FIPS 140 Level 2 hardware security module.	For the medium H/W level of assurance, the Identity shall be established by in-person proofing before the Registration Authority or the Trusted Agent; information provided shall be verified to ensure legitimacy. A trust relationship between the Trusted Agent and the applicant which is based on an in-person antecedent may suffice as meeting the in-person identity proofing requirement. Credentials required are one Federal Government-issued Picture I.D., one REAL ID Act compliant picture ID1, or two Non-Federal Government I.D.s, one of which shall be a photo I.D. (e.g., Non-REAL ID Act compliant Drivers License). Any credentials presented must be unexpired.  Clarification on the trust relationship between the Trusted Agent and the applicant, which is based on an in-person antecedent identity proofing event, can be found in the "FBCA Supplementary Antecedent, In-Person Definition" document.
High / treasury-level 5 {2 16 840 1 101 3 2 1 5 5}	This level is reserved for use by Government employees and is appropriate for those environments where the threats to data are high, or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.	For this level of assurance, identity established by in-person appearance before the Registration Authority or Trusted Agent; information provided shall be checked to ensure legitimacy. Credentials required are either one Federal Government-issued Picture I.D., or two Non-Federal Government I.D.s, one of which shall be a photo I.D. (e.g., Drivers License).
PIV-I Hardware / treasury-pivi-hardware {TBD}	This policy is reserved for use on a PIV-I Card and provides strong assurance of security. Depending on the key usage and PIV-I Card container, the certificate could be used for authentication, digital signature, or encryption.	For PIV-I Hardware, credentials required are two identity source documents in original form. The identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 1115-0136, Employment Eligibility Verification. At least one document shall be a valid State or Federal Government-issued picture identification (ID). For PIV-I, the use of an in-person antecedent is not applicable.
PIV-I Card Authentication / treasury-pivi-cardAuth {2 16 840 1 101 3 2 1 5 11}	This level is used to uniquely identify a PIV-I card – not the cardholder – for the purposes granting the cardholder physical access to high-volume, low-risk areas or in combination with	For PIV-I Card Authentication, credentials required are two identity source documents in original form. The identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 1115-0136, Employment Eligibility Verification. At least one document shall be a valid State or Federal

**UNCLASSIFIED**

Certificate Policy / OID	Description	Identity Proofing
	other authentication mechanisms for access to high-risk areas.	Government-issued picture identification (ID). For PIV-I, the use of an in-person antecedent is not applicable.
PIV-I Content Signing / treasury-pivi-contentSigning {2 16 840 1 101 3 2 1 5 12}	This policy is reserved for use by any CMS that manages PIV-I cards to sign containers on the cards. Special requirements are placed on the CMS to ensure that the keys are highly protected and secure.	For PIV-I content signing, sponsor credentials required are two identity source documents in original form. The identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 1115-0136, Employment Eligibility Verification. At least one document shall be a valid State or Federal Government-issued picture identification (ID). For PIV-I, the use of an in-person antecedent is not applicable.
Common Software / id-fpki-common-policy {2 16 840 1 101 3 2 1 3 6}	Common Software / id-fpki-common-policy ::= {2 16 840 1 101 3 2 1 3 6}	The applicant presents a government issued ID to an RA or a Trusted Agent. The ID is either verified against a database or is corroborated by a second form of identification. A biometric of the applicant must be captured.
Common Hardware / id-fpki-common-hardware {2 16 840 1 101 3 2 1 3 7}	This level is reserved for use by Government employees and contractors. It is appropriate for unclassified data environments.	The applicant presents a government issued ID to an RA or a Trusted Agent. The ID is either verified against a database or is corroborated by a second form of identification. A biometric of the applicant must be captured.
Common Devices / id-fpki-common-devices {2 16 840 1 101 3 2 1 3 8}	This level is reserved for use by Government sponsored- devices. It is appropriate for unclassified data environments.	The applicant presents a government issued ID to an RA or a Trusted Agent. The ID is either verified against a database or is corroborated by a second form of identification. A biometric of the applicant must be captured.
Common Hardware Devices / id-fpki-common-devicesHardware {2 16 840 1 101 3 2 1 3 36}	This level is reserved for use by Government sponsored- devices. It is appropriate unclassified for data environments.	The applicant presents a government issued ID to an RA or a Trusted Agent. The ID is either verified against a database or is corroborated by a second form of identification. A biometric of the applicant must be captured.
Common Authentication / id-fpki-common-authentication {2 16 840 1 101 3 2 1 3 13}	This level is reserved for use by Government employees and contractors. It is appropriate for unclassified data environments.	The applicant presents a government issued ID to an RA. The ID is either verified against a database or is corroborated by a second form of identification. A biometric of the applicant must be captured.
Common High / id-fpki-common-high {2 16 840 1 101 3 2 1 3 16}	This policy is reserved for subscribers who are Federal employees. It is suitable for high-value transactions where there is a desire for assurance that the user is a Federal employee.	At id-fpki-common-High, the applicant shall appear at the RA in person. The applicant presents a government issued ID that is either verified against a database or is corroborated by a second form of identification. A biometric of the applicant must be captured.
Common Card Authentication / id-fpki-common-cardAuth {2 16 840 1 101 3 2 1 3 17}	This level is used to uniquely identify a PIV card – not the cardholder – for the purposes granting the cardholder physical access to high-volume, low-risk areas or in combination with other authentication mechanisms for access to high-risk areas.	The applicant presents a government issued ID to an RA. The ID is either verified against a database or is corroborated by a second form of identification. A biometric of the applicant must be captured.

## APPENDIX E BIBLIOGRAPHY

The following documents contain information that is required by reference or that otherwise describes or governs Department of the Treasury PKI operation:

Reference	Title
36 CFR	Subchapter B Records Management Part 1220 Federal Records
ABADSG	Digital Signature Guidelines, 1996-08-01. <a href="http://www.abanet.org/scitech/ec/isc/dsgfree.html">http://www.abanet.org/scitech/ec/isc/dsgfree.html</a>
COMMON CP	X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework, Version 1.30, October 4, 2018
FBCA CP	X.509 Certificate Policy For The Federal Bridge Certificate Authority, Version 2.34, October 5, 2018
FED KRP	Federal Public Key Infrastructure Key Recovery Policy, Version 1, October 6, 2017
FIPS 201	Personal Identity Verification (PIV) of Federal Employees and Contractors
FIPS 140-1	Security Requirements for Cryptographic Modules, 1994-01
FIPS 140-2	Security Requirements for Cryptographic Modules May 25, 2001. <a href="http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf">http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf</a>
FIPS 186	Digital Signature Standard, 1994-05-19
FIPS 186-2	Digital Signature Standard, January 27, 2000. <a href="http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf">http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf</a>
FOIACT	5 U.S.C. 552, Freedom of Information Act. <a href="Http://www4.law.cornell.edu/uscode/5/552.html">Http://www4.law.cornell.edu/uscode/5/552.html</a> FPKI-E
FPKI-PROF	Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile, Version 1.9, May 10, 2018
ISO9594-8	Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, 1997
ITMRA	Public Law 104-106 Division E - Information Technology Management Reform 40 U.S.C. 1452, Information Technology Management Reform Act of 1996. <a href="Http://www4.law.cornell.edu/uscode/40/1452.html">Http://www4.law.cornell.edu/uscode/40/1452.html</a> NAG69C NAG69C
NIST SP 800-73	Interfaces for Personal Identity Verification (4 Parts) <a href="http://csrc.nist.gov/publications/PubsSPs.html">http://csrc.nist.gov/publications/PubsSPs.html</a>
NIST SP 800-76	Biometric Data Specification for Personal Identity Verification <a href="http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf">http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf</a>
NIST SP 800-78	Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV). <a href="http://csrc.nist.gov/publications/nistpubs/800-78-2/sp800-78-2.pdf">http://csrc.nist.gov/publications/nistpubs/800-78-2/sp800-78-2.pdf</a>
CNSSI 4005	CNSSI 4005, Safeguarding COMSEC Facilities and Material, August 2011.
CNSSI 4009	CNSSI 4009, Committee on National Security Systems (CNSS) Glossary, April 2015.
NSD42	National Policy for the Security of National Security Telecom and Information. <a href="Http://snyside.sunnyside.com/cpsr/privacy/computer_security/ns_d_42.txt">Http://snyside.sunnyside.com/cpsr/privacy/computer_security/ns_d_42.txt</a> (redacted version)
PA	5 U.S.C. 552a Privacy Act, 1974, as amended

UNCLASSIFIED

Reference	Title
PIV-I PROF	X.509 Certificate and CRL Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards, Version 1.3, May 10, 2018
PKCS #12	Personal Information Exchange Syntax Standard, April 1997. <a href="ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf">ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf</a>
RFC 4210	Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP), Adams, Farrell, Kaue and Mononen, Sep 2005
RFC 3647	Certificate Policy and Certification Practices Framework, Chokhani, Ford, Sabett, Merrill, and Wu, November 2003.
SSP-PROF	X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program, Version 1.9, May 9, 2018

## APPENDIX F      ACRONYMS AND ABBREVIATIONS

The following acronyms and abbreviations appear in this certificate policy and are applicable to the Department of the Treasury PKI operation:

Acronym	Expression
AIS	Automated Information System
ARL	Authority Revocation List
CA	Certification Authority
CARL	Certificate Authority Revocation List
CIO	Chief Information Officer
CISA	Certified Information System Auditor
CMA	Certificate Management Authority
CMS	Card Management System
COMSEC	Communications Security
COTS	Commercial off-the-shelf
CP	Certificate Policy
CPF	Common Policy Framework
CPS	Certification Practices Statement
CRL	Certificate Revocation List
CSA	Certificate Status Authority
CSOR	Computer Security Object Registry
CSS	Certificate Status Servers
CUI	Controlled Unclassified Information
DC	Domain Component
DN	Distinguished Name
DSS	Digital Signature Standard
FBCA	Federal Bridge Certification Authority
FCPF	Federal Common Policy Framework
FIPS	Federal Information Processing Standards
FPKI-E	Federal PKI Version 1 Technical Specifications: Part E – X.509 Certificate and CRL Extensions Profile
FPKIPA	Federal PKI Policy Authority
GS	General Schedule (Federal civilian level)
HSM	Hardware Security Module
HTTP	HyperText Transfer Protocol
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ISSO	Information Systems Security Officer
KRP	Key Recovery Policy

**UNCLASSIFIED**

<b>Acronym</b>	<b>Expression</b>
KRPS	Key Recovery Practice Statement
LDAP	Lightweight Directory Access Protocol
LRA	Local Registration Authority
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NSA	National Security Agency
NIST	National Institute of Standards and Technology
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OCIO	Office of the Chief Information Officer
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PCA	Principal Certification Authority
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification – Interoperable
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PMA	Policy Management Authority
PMO	Program Management Office
RA	Registration Authority
SHA-X	Secure Hash Algorithm (X: indicates the version number, e.g., Version 1, Version 256)
SSP	Share Service Provider
TPKI	Treasury Public Key Infrastructure
TD P	Treasury Department Publication
TRCA	Treasury Root Certification Authority
U.S.C.	United States Code
UPN	User Principal Name
URL	Uniform Resource Locator
UUID	Universally Unique Identifier (defined by RFC 4122)
VME	Virtual Machine Environment
WWW	World Wide Web

## APPENDIX G GLOSSARY

The following terms appear in this certificate policy and are applicable to the Department of the Treasury PKI operation:

Term	Definition
Access	Ability to make use of any information system (IS) resource. NSTISSI 4009
Access Control	Process of granting access to information system resources only to authorized Subscribers, 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).
Affiliated Organization	Organizations that authorize affiliation with Subscribers of PIV-I certificates
Applicant	The Subscriber, sometimes also called an "applicant," after applying to a Certification Authority for a certificate, but before the certificate issuance procedure is completed. ABSG footnote 32
Archive	Long-term, physically separate storage.
Attribute Authority	An Entity, recognized by the FPKIPA or comparable Entity 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]

**UNCLASSIFIED**

<b>Term</b>	<b>Definition</b>
Binding	Process of associating two related elements of information. [NS4009]
Biometric	A physical or behavioral characteristic of a human being.
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 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.
Certificate Management Authority (CMA)	A Certification Authority or a Registration Authority.
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 applications.
Certificate Revocation List (CRL)	A list maintained by a Certification Authority of the certificates, which it has issued, 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.
Certificate-Related Information	Information, such as a Subscriber's postal address, that is not included in a certificate, but that a CA may use in certificate management.
Certification Authority (CA)	An authority trusted by one or more Subscribers to issue and manage X.509 Public Key Certificates and ARLs or CRLs.
Certification Authority Revocation List (ARL)	A signed, time-stamped list of serial numbers of CA public key certificates, including cross certificates that have been revoked.
Certification Authority Software	Key Management and cryptographic software used to manage certificates issued to Subscribers.

**UNCLASSIFIED**

Term	Definition
Certification Practice 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).
Client (application)	A system Entity, usually a computer process acting on behalf of a human Subscriber 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.
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. [FIPS1401]
Crypto-period	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, which 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 Entity as defined above.

**UNCLASSIFIED**

<b>Term</b>	<b>Definition</b>
Encrypted Network	A network that is protected from outside access by National Security Agency (NSA) approved high-grade (Type I) cryptography.
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	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.
Entity CA	A CA that acts on behalf of an Entity, and is under the operational control of an Entity.
FBCA Operational Authority (FBCA OA)	The Federal Public Key Infrastructure 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 (FPKIPA)	The FPKIPA is a federal government body responsible for setting, implementing, and administering policy decisions regarding inter-Entity PKI interoperability, the FBCA, and the Federal Common Policy Framework.
Firewall	Gateway that limits access between networks in accordance with local security policy. [NS4009]
High Assurance Guard (HAG)	An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.
Hypervisor	Computer software, firmware or hardware that creates and runs virtual machines. A hypervisor uses native execution to share and manage hardware, allowing for multiple environments which are isolated from one another, yet exist on the same physical machine. Also known as an isolation kernel or virtual machine monitor. (See Virtual Machine Environment)
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.

**UNCLASSIFIED**

<b>Term</b>	<b>Definition</b>
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 Management Key	The private key associated with a PKI certificate that asserts only Key Encypherment or Key Agreement in the certificate Key Usage field.
Key Pair	Two mathematically related keys having the properties that (i) 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 FPKIPA and an Entity allowing interoperability between the Entity Principal CA and the Federal PKI.
Mission Critical Information	Information deemed vital to the operational readiness or mission effectiveness of deployed and contingency forces, in terms of context and timeliness.
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.

**UNCLASSIFIED**

Term	Definition
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 identify uniquely each of the 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)	Entity established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies. For the FBCA, the PMA is the FPKIPA.
Principal CA	The Principal CA is a CA designated by an Entity to interoperate with the FBCA.

**UNCLASSIFIED**

<b>Term</b>	<b>Definition</b>
Privacy	Restricting access to Subscriber or Relying Party information in accordance with Federal law and Entity policy.
Private Key	The key of an asymmetric encryption algorithm that is protected from disclosure.
Public Key	The key of an asymmetric encryption algorithm made publicly available normally in the form of a digital certificate. (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.
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 Entity 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 harmful result.
Risk Tolerance	The level of risk an Entity is willing to assume to achieve a potential desired result.
TRCA	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.

**UNCLASSIFIED**

<b>Term</b>	<b>Definition</b>
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	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).
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
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]
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 Entity 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.

UNCLASSIFIED

Term	Definition
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.
Virtual Machine Environment	An emulation of a computer system (in this case, a CA) that provides the functionality of a physical machine in a platform-independent environment. They provide functionality needed to execute entire operating systems. (See Hypervisor)
Zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS1401]

## **APPENDIX H      ACKNOWLEDGEMENTS**

The Department of the Treasury Public Key Infrastructure/Policy Management Authority developed this CP based on the existing Department of the Treasury PKI CP as well as RFC 3647, U.S. Federal PKI Common Policy Framework Certificate Policy and the FBCA Certificate Policy.