X.509 Certificate Policy

For The

US Treasury PKI

TREASURY PKI PMO/PMA

Version 1.4

August 29, 2002

Table of Contents

1. INTRODUCTION 1

1.1 OVERVIEW 1

1.1.1 Certificate Policy (CP) 1

1.2 IDENTIFICATION 1

1.3 COMMUNITY AND APPLICABILITY 2

1.3.1 PKI Authorities 2

1.3.2 Related Authorities 3

1.3.3 End Entities 3

1.3.4 Applicability 3

1.4 CONTACT DETAILS 3

1.4.1 Specification Administration Organization 3

1.4.2 Contact Person 4

1.4.3 Person Determining Certification Practice Statement Suitability 4

2. GENERAL PROVISIONS 5

2.1 OBLIGATIONS 5

2.1.1 CA Obligations 5

2.1.2 RA Obligations 5

2.1.3 Subscriber Obligations 6

2.1.4 Relying Party Obligations 6

2.1.5 Repository Obligations 6

2.2 REQUIREMENTS FOR ISSUING CERTIFICATES TO NON-US GOVERNMENT PARTIES 7

2.2.1 Liability 7

2.2.2 Governing Law 7

2.2.3 Administrative Processes 7

2.3 INTERPRETATION AND ENFORCEMENT 8

2.3.1 Severability of Provisions, Survival, Merger, and Notice 8

2.3.2 Dispute Resolution Procedures 8

2.4 PUBLICATION AND REPOSITORY 8

2.4.1 Publication of CA Information 8

2.4.2 Frequency of Publication 8

2.4.3 Access Controls 8

2.4.4 Repositories 8

2.5 COMPLIANCE AUDIT 8

2.5.1 Frequency of Entity Compliance Audit 9

2.5.2 Identity/Qualifications of Compliance Auditor 9

2.5.3 Compliance Auditor's Relationship to Audited Party 9

2.5.4 Topics Covered by Compliance Audit 9

2.5.5 Actions Taken as a Result of Deficiency 9

2.5.6 Communication of Result 9

2.6 CONFIDENTIALITY 10

2.6.1 Types of Information to be Protected 10

2.6.2 Information Release Circumstances 10

2.7 INTELLECTUAL PROPERTY RIGHTS 10

2.8 FEES 10

3. IDENTIFICATION AND AUTHENTICATION 11

3.1 INITIAL REGISTRATION 11

3.1.1 Types of Names 11

3.1.2 Need for Names to be Meaningful 11

3.1.3 Rules for Interpreting Various Name Forms 11

3.1.4 Uniqueness of Names 11

3.1.5 Name Claim Dispute Resolution Procedure 12

3.1.6 Recognition, Authentication and Role of Trademarks 12

3.1.7 Method to Prove Possession of Private Key 12

3.1.8 Authentication of Organization Identity 12

3.1.9 Authentication of Individual Identity 12

3.1.10 Authentication of Component Identities 13

3.2 CERTIFICATE RENEWAL, UPDATE, AND ROUTINE RE-KEY 14

3.2.1 Certificate Re-key 14

3.2.2 Certificate Renewal 14

3.2.3 Certificate Update 15

3.3 OBTAINING A NEW CERTIFICATE AFTER REVOCATION 15

3.4 REVOCATION REQUEST 15

4. OPERATIONAL REQUIREMENTS 16

4.1 CERTIFICATE APPLICATION 16

4.1.1 Delivery of Subscriber Public Key to Certificate Issuer 16

4.2 CERTIFICATE ISSUANCE 17

4.2.1 Delivery of Subscriber's Private Key to Subscriber 17

4.2.2 CA Public Key Delivery to Subscribers 17

4.3 CERTIFICATE ACCEPTANCE 18

4.4 CERTIFICATE SUSPENSION AND REVOCATION 18

4.4.1 Revocation 18

4.4.2 Suspension 19

4.4.3 Certificate Revocation Lists 19

4.4.4 On-line Revocation / Status Checking Availability 20

4.4.5 Other Forms of Revocation Advertisements Available 20

4.4.6 Checking Requirements for Other Forms of Revocation Advertisements 20

4.4.7 Special Requirements Related to Key Compromise 20

4.5 SECURITY AUDIT 20

4.5.1 Types of Events Recorded 21
4.5.2 Audit Processing Frequency 25
4.5.3 Retention Period for Audit Data 26
4.5.4 Protection of Audit Data 26
4.5.5 Audit Data Backup Procedures 27
4.5.6 Audit Collection System (internal vs. external) 27
4.5.7 Notification to Audit Event-causing Subject 27
4.5.8 Vulnerability Assessments 27
4.6 RECORDS ARCHIVAL 27
4.6.1 Types of Events Archived 27
4.6.2 Retention Period for Archive 28
4.6.3 Protection of Archive 28
4.6.4 Archive Backup Procedures 28
4.6.5 Requirements for Time-stamping Archive Records 29
4.6.6 Archive Collection System (internal or external) 29
4.6.7 Procedures to Obtain and Verify Archive Information 29
4.7 KEY CHANGEOVER 29
4.8 COMPROMISE AND DISASTER RECOVERY 29
4.8.1 Computing Resources, Software, and/or Data 29
4.8.2 Private Key Compromise 29
4.8.3 Facility Disaster 30
4.9 CA TERMINATION 30
5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS 31
5.1 PHYSICAL CONTROLS 31
5.1.1 Site Location and Construction 31
5.1.2 Physical Access 31
5.1.3 Electrical Power 32
5.1.4 Water Exposures 32
5.1.5 Fire Prevention and Protection 32
5.1.6 Media Storage 32
5.1.7 Waste Disposal 32
5.1.8 Off-site Backup 32
5.2 PROCEDURAL CONTROLS 33
5.2.1 Trusted Roles 33
5.2.2 Separation of Roles 34
5.2.3 Number of Persons Required per Task 35
5.2.4 Identification and Authentication for Each Role 35
5.3 PERSONNEL CONTROLS 35
5.3.1 Background, Qualifications, Experience, and Security Clearance Requirements 35

5.3.2 Background Check Procedures 35
5.3.3 Training Requirements 35
5.3.4 Retraining Frequency and Requirements 35
5.3.5 Job Rotation Frequency and Sequence 35
5.3.6 Sanctions for Unauthorized Actions 36
5.3.7 Contracting Personnel Requirements 36
5.3.8 Documentation Supplied to Personnel 36

6. TECHNICAL SECURITY CONTROLS 37

6.1 KEY PAIR GENERATION AND INSTALLATION 37
6.1.1 Key Pair Generation 37
6.1.2 Private Key Delivery to Subscriber 37
6.1.3 Subscriber Public Key Delivery to Certificate Issuer 37
6.1.4 CA Public Key Delivery to Subscribers 37
6.1.5 Key Sizes 37
6.1.6 Public Key Parameters Generation 38
6.1.7 Parameter Quality Checking 38
6.1.8 Hardware/Software Key Generation 38
6.1.9 Key Usage (as per X.509 v3 key usage field) 38

6.2 PRIVATE KEY PROTECTION 38
6.2.1 Standards for Cryptographic Modules 38
6.2.2 CA Private Key Multi-person Control 39
6.2.3 Private Key Escrow 39
6.2.4 Private Key Backup 39
6.2.5 Private Key Archival 39
6.2.6 Private Key Entry into Cryptographic Module 39
6.2.7 Method of Activating Private Key 40
6.2.8 Methods of Deactivating Private Key 40
6.2.9 Method of Destroying Private Signature Key 40

6.3 PRACTICES REGARDING KEY-PAIR MANAGEMENT 40
6.3.1 Public Key Archival 40
6.3.2 Usage Periods for the Public and Private Keys 40

6.4 ACTIVATION DATA 40
6.4.1 Activation Data Generation and Installation 40
6.4.2 Activation Data Protection 41
6.4.3 Other Aspects of Activation Data 41

6.5 COMPUTER SECURITY CONTROLS 41
6.5.1 Specific Computer Security Technical Requirements 41
6.5.2 Computer Security Rating 41

6.6 LIFE-CYCLE TECHNICAL CONTROLS *42*
6.6.1 Security Management Controls 42
6.6.2 Life Cycle Security Ratings 42
6.7 NETWORK SECURITY CONTROLS *42*
6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS *42*
7. CERTIFICATE AND CRL PROFILES **43**
7.1 CERTIFICATE PROFILE *43*
7.1.1 Version Numbers 43
7.1.2 Certificate Extensions 43
7.1.3 Algorithm Object Identifiers 43
7.1.4 Name Forms 44
7.1.5 Name Constraints 44
7.1.6 Certificate Policy Object Identifier 44
7.1.7 Usage of Policy Constraints extension 44
7.1.8 Policy Qualifiers Syntax and Semantics 44
7.1.9 Processing Semantics for Critical Certificate Policy Extension 44
7.2 CRL PROFILE *44*
7.2.1 Version Number 44
7.2.2 CRL and CRL Entry Extensions 44
8. SPECIFICATION ADMINISTRATION **45**
8.1 SPECIFICATION CHANGE PROCEDURES *45*
8.2 PUBLICATION AND NOTIFICATION POLICIES *45*
8.3 CPS APPROVAL PROCEDURES *45*
8.4 WAIVERS *45*
9. BIBLIOGRAPHY **46**
10. ACRONYMS AND ABBREVIATIONS **48**

RECORD OF CHANGES

Change Number	Date of Change	Reason for Change	SIGNATURE OF PERSON ENTERING CHANGE
1.2	May 20, 2002	To reflect revised operation environment	Bernadette A. Curry
1.3	July 31, 2002	To meet the requirements of the Federal Policy Management Certificate Policy Management Working Group for Cross Certification with the Federal Bridge	Bernadette A. Curry
1.4	August 29, 2002	To specify that the Treasury Root CA will issue CRLs monthly for cross-certification purposes with the FBCA	Bernadette A. Curry

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 Treasury.

This Certificate Policy (CP) defines four certificate policies for use by the United States Treasury Department Office of the Chief Information Officer (OCIO) Public Key Infrastructure (PKI). The OCIO PKI consists of the Treasury Root CA, the Treasury Operational CA (OCA), subordinate bureau CAs, and the Registration Authorities (RAs) and Local Registration Authorities (LRAs) and subscribers associated with these CAs.[1] This CP apply to all the CAs, RAs, LRAs, and users of the OCIO PKI, including the Treasury Root Certification Authority (CA), the Treasury OCA and subordinate bureau CAs.

These CPs are based on the Federal Bridge Certification Authority (FBCA) CPs and the Treasury Security Manual TDP 71-10, Chapter 6, Section 4.D.4 and 4.D.4.S, "Public Key Infrastructure policy" and "Public Key Infrastructure Standards". The OCIO PKI certificates will assert the FBCA Object Identifiers (OIDs). The four CPs represent four different assurance levels: Level 1, Level 2, Level 3, and Level 4. These four assurance levels are intended to map to the FBCA assurance levels. The word "assurance" used in this CP means how well a Relying Party can be certain of the identity binding between the public key and the individual whose subject name is cited in the certificate. In addition, it also reflects how well the Relying Party can be certain that the individual whose subject name is cited in the certificate is controlling the use of the private key that corresponds to the public key in the certificate.

The OCIO PKI will consist of the Treasury Root CA that is off-line, the Treasury OCA which is online and operational and Bureau CAs. The Treasury OCA and Bureau CAs are subordinate to the Root CA. In addition, the Root CA will act the Principal CA (PCA) for the FBCA. The Treasury Root CA will also act as the Bridge CA (BCA) for the Treasury bureaus and agencies that have their own roots and wish to cross certify with the OCIO PKI in order to interoperate with the OCIO PKI and with the Federal PKI.

1.1 Overview

1.1.1 Certificate Policy (CP)

As stated this document contains CPs for four assurance levels. Each of the assurance level CP addresses both the digital signature verification public key certificates and the key management public key certificates. The reliance a bureau will choose to place on a given level of certificate assurance will be based on: 1) the amount and type of inherent risk of an activity; 2) the consequence of failure; and 3) the use of risk mitigation controls.

1.2 Policy Identification

The US Treasury Root CA operates at several levels of assurance. These levels of assurance have object identifiers (OIDs), to be asserted in certificates issued by the US Treasury Root CA. To allow for the addition of assurance levels in the future, the OID will be registered under the id-certificate-policy arc as follows:

Treasury-policies ID ::= {2 16 840 1 101 3 2 1 5}

[1] Treasury bureaus may have CAs that are not subordinate to the OCIO root CA. These CAs are not considered part of the OCIO PKI. These CAs may choose to follow or not follow the CPs described in this document.

Treasury Rudimentary Assurance	ID ::= treasury-cp1 2
Treasury Basic Assurance	ID ::= treasury-cp2 3
Treasury Medium Assurance	ID ::= treasury-cp3 4
Treasury High Assurance	ID ::= treasury-cp4 5

1.3 Community and Applicability

1.3.1 PKI Authorities

1.3.1.1

The Treasury PKI PMO resides in the Office of Customer Service Infrastructure Operations (CSIO), Office of the Chief Information Officer (OCIO).

The Treasury PMO is responsible for:

- Creation, publication and maintenance of all CP and CPS pertaining to the US Treasury PKI;
- Acceptance of applications from Agencies and Bureaus for certification of their subordinate CAs;
- Management of the Treasury OCA;
- Bureau RA and LRA training
- Bureau RA and LRA guidance
- Determination regarding CP and CPS compliance and assurance level with the US Treasury CP.

1.3.1.2.

The Policy Management Authority (PMA) also resides in the OCIO. The PMA is primarily responsible for:

- Creation and publication of all Treasury PKI Policy,
- Review and approval of a CP and CPS pertaining to CAs being considered for cross certification with the US Treasury Root CA.

1.3.1.2 Treasury Root CA

The Treasury root CA shall be housed and maintained by the Department of the Treasury OCIO. The Treasury Root CA shall be kept off-line and shall not be connected to any network. The Treasury Root CA shall also act as the Principal CA (PCA) for the Treasury. The Treasury Root CA shall cross-certify with the Federal Bridge Certification Authority (FBCA), Treasury bureau CAs that are not subordinate to the Treasury Root CA and non Treasury CAs. The Treasury Root CA shall also certify the Treasury agencies and bureaus CAs that want to be part of the hierarchy (as opposed to cross-certification).

1.3.1.3 Agencies and Bureaus CAs

Agencies and bureaus shall be responsible for the operation of subordinate CAs established as part of the OCIO PKI in accordance with one or more assurance levels CPs described in this document.

1.3.1.4 Registration Authority (RA)

The RA is the entity that collects and verifies each Subscriber's identity and information that are to be entered into his or her public key certificate. The RA may delegate this responsibility to a LRA.

1.3.1.5 Repository

The repository shall contain certificates, Certificate Revocation Lists (CRLs) and CP and CPS.

1.3.2 Related Authorities

1.3.2.1 Federal Bridge Certification Authority (FBCA)

The FBCA is the CA operated by the FBCA OA and issues certificates to the various US Federal Department and agencies PCAs.

1.3.3 End Entities

1.3.3.1 Subscribers

Subscribers for the OCIO PKI shall consist of the human users and non-human system components. The human subscribers shall consist of authorized Treasury personnel and authorized contractor personnel. The non-human system components shall consist of the Treasury computers and other Information Technology related machines that require public key certificates.

1.3.3.2 Relying Parties

Relying parties shall consist of all the subscribers and personnel and machines from US Government agencies and private sector that have need for secure communication with the US Treasury.

1.3.3.3 PKI Sponsor

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

1.3.4 Applicability

The sensitivity of the information processed or protected using certificates issued by OCIO PKI will vary significantly. The reliance a bureau will choose to place on a given level of certificate assurance will be based on: 1) the amount and type of inherent risk of an activity; 2) the consequence of failure; and 3) the use of risk mitigation controls.

1.4 Contact Details

1.4.1 Specification Administration Organization

The Treasury PKI PMO is responsible for all aspects of this CP.

1.4.2 Contact Person

Questions regarding this CP shall be directed to the Chair of the Treasury PKI PMO whose address is:

Treasury PKI PMO, CSIO, RM 12113, 1750 Pennsylvania Ave, NW, Washington DC 20220

1.4.3 Person Determining Certification Practice Statement Suitability

The Treasury PKI PMO shall approve all Treasury CPS claiming compliance with the CPs in this document.

2. GENERAL PROVISIONS

2.1 Obligations

2.1.1 CA Obligations

A CA that is part of the OCIO PKI shall conform to the stipulations of this document, including:

- providing to the Treasury PKI PMO a CPS, as well as any subsequent changes, for conformance assessment;
- conforming to the stipulations of the approved CPS;
- ensuring that registration information is accepted only from RAs and or LRAs who understand and are obligated to comply with this policy;
- including only valid and appropriate information in the certificate, and to maintain evidence that due diligence was exercised in validating the information contained in the certificate;
- ensuring that obligations are imposed on Subscribers in accordance with Section 2.1.3, and informed of the consequences of not complying with those obligations,
- revoking the certificates of Subscribers found to have acted in a manner counter to their obligations;
- ensuring that obligations are imposed on non-US Government Subscribers in accordance with the provisions of Section 2.2; and
- operating or providing for the services of an on-line repository that satisfies the obligations under Section 2.1.5, and informing the repository service provider of those obligations if applicable.

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

2.1.2 RA Obligations

A RA who performs registration functions as described in this document shall comply with the stipulations of this document, and comply with the pertinent CPS approved by the Treasury PMO for use with this policy. A RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities.

RA(s) shall be responsible for obtaining registration or revocation information from users, authenticating users, and forwarding the results to the CA. RAs may delegate user registration and authentication to LRAs.

2.1.3. LRA Obligations

A LRA who performs registration functions as described in this document shall comply with the stipulations of this document, and comply with the pertinent CPS approved by the Treasury PMO for use

with this policy. A LRA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of LRA responsibilities.

2.1.3 Subscriber Obligations

- Subscribers are responsible for notifying, in a timely manner, the CA that issued their certificates of suspicion that their private keys are compromised or lost. Such notification shall be made directly, or indirectly through mechanisms consistent with the CA's CPS;
- Requesting revocation of a certificate if a key is no longer needed;
- Memorizing and not recording any passwords or PINs associated with private keys or eventual use of tokens;
- Protecting their private keys and cryptographic tokens at all times, in a manner similar to a building pass or official credentials;
- Ensuring that workstations are not left in an unattended/unlocked state when a certificate has been used for system access.
- Using certificates provided by the OCIO PKI only for transactions related to Treasury business or such additional transactions as are provided for in a written subscriber agreement.
- Representing themselves accurately in all communications with the PKI; and
- Abiding by all the terms, conditions, and restrictions levied upon the use of their private keys and certificates.

PKI Sponsors assume the obligations of Subscribers for the certificates associated with their components.

2.1.4 Relying Party Obligations

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

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

Relying parties who verify certificates using Certificate Status Authorities (CSA) shall only use CSAs approved by the Treasury PMO.

2.1.5 Repository Obligations

Repositories that support a CA in posting information as required by this policy shall:

- maintain availability of the information as required by the certificate information posting and retrieval stipulations of this policy;

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

2.2 Requirements For Issuing Certificates To Non-Us Government Parties

OCIO PKI may issue certificates to parties other than agencies, officers and employees of the U.S. Government, such as contractors and parties regulated by Treasury, for the convenience of the Government when those parties have a bona fide need to securely communicate with Treasury agencies and bureaus. OCIO PKI shall impose the stipulations of this section upon Subscribers by including the following provisions in the Subscriber agreements.

2.2.1 Liability

The United States Government disclaims any liability that may arise from use of any certificate issued by the OCIO PKI, or the OCIO PKI determination to revoke a certificate issued by the OCIO PKI. In no event will the U.S. Government be liable for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to any certificate issued by the OCIO PKI.

The United States Government disclaims any liability that may arise from the use of the CPs in this document.

2.2.1.1 Financial Considerations

This CP contains no limits on the use of any certificates, issued by the OCIO PKI. Rather, agencies, acting as Relying Parties, shall determine what financial limits, if any, they wish to impose for certificates used to consummate a transaction.

All financial issues shall be covered by the Federal Claims and Tort Act.

2.2.1.2 Indemnification by Relying Parties and Subscribers

All financial issues shall be covered by the Federal Claims and Tort Act.

2.2.1.3 Fiduciary Relationships

No stipulation.

2.2.2 Governing Law

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

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

2.2.3 Administrative Processes

Administrative processes pertaining to this CP shall be determined by the Treasury PMO.

2.3 Interpretation And Enforcement

2.3.1 Severability of Provisions, Survival, Merger, and Notice

Should it be determined that one section of this CP is incorrect or invalid, the other section of this CP shall remain in effect until the CP is updated. The process for updating this CP is described in section 8.1

2.3.2 Dispute Resolution Procedures

The Treasury PMO shall resolve any disputes associated with the use of the certificates issued by the OCIO PKI.

2.4 Publication And Repository

2.4.1 Publication of CA Information

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

- issued certificates;
- a CRL;
- the CA's certificate for its certificate signing key;
- a copy of this Policy, including any waivers granted to the CA by the Treasury PMO; and
- a copy of the Subscriber duties and responsibilities.

2.4.2 Frequency of Publication

Certificates shall be published as specified in section 3.2. Certificate status information shall be published as specified in section 4.4.3.1. All information to be published in the repository shall be published promptly after such information becomes available to the CA. The CA shall specify in its CPS time limits within which it will publish various types of information.

2.4.3 Access Controls

A CA shall protect any repository information not intended for public dissemination or modification. Public key certificates and certificate status information in the repository shall be publicly available.

2.4.4 Repositories

The location of any repository shall be one which provides access to Subscribers and Relying Parties in accordance with the security requirements stipulated in this document.

2.5 Compliance Audit

All CAs, RAs and LRAs shall have a compliance audit mechanism in place to ensure that they are operating in accordance with their CPS.

2.5.1 Frequency of Entity Compliance Audit

All CAs shall be subject to a periodic compliance audit which is no less frequent than once per year for Assurance Levels 3 and 4, and no less than once every two years for Assurance Level 2. There is no audit requirement for CAs, RAs and LRAs operating at the Assurance Level 1.

A CA 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 OCIO PKI.

2.5.2 Identity/Qualifications of Compliance Auditor

The auditor must demonstrate competency in the field of compliance audits, and must be thoroughly familiar with the CA,the RA and LRA CPS. The compliance auditor must perform such compliance audits as a primary responsibility. The CPS shall identify the compliance auditor.

2.5.3 Compliance Auditor's Relationship to Audited Party

The compliance auditor either shall be the Treasury PMA or a private firm selected by the Treasury PMA. The private firm shall be independent from the entity being audited, or it shall be sufficiently organizationally separated from that entity to provide an unbiased, independent evaluation.

2.5.4 Topics Covered by Compliance Audit

The purpose of a compliance audit shall be to verify that an entity subject to the requirements of this CP and its CPS **is complying with the requirements of those documents**. All aspects of the entity (CA, RA, LRA) operation related to this CP shall be subject to compliance audit.

2.5.5 Actions Taken as a Result of Deficiency

When the compliance auditor finds a discrepancy between how the entity being audited is designed or is being operated or maintained, and the requirements of this CP and the entity's CPS, the following actions shall be taken:

- The compliance auditor shall note the discrepancy;
- The compliance auditor shall notify the parties identified in Section 2.5.6 of the discrepancy; and
- The entity being audited shall propose a remedy, including expected time for completion to the Treasury PMO.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the Treasury PMO may decide to halt temporarily operation of the entity, to revoke a certificate issued to the entity, or take other actions it deems appropriate. Upon correction of the deficiency, the Treasury PMO may reinstate the entity.

2.5.6 Communication of Result

The compliance auditor shall report the results of a compliance audit to the Treasury PMA,PMO and the Treasury CIO. The results will be reported to the audited entity. The implementation of remedies shall be communicated to the Treasury PMO. A special compliance audit may be required to confirm the implementation and effectiveness of the remedy.

2.6 Confidentiality

2.6.1 Types of Information to be Protected

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

Special procedures may be necessary to deal with aggregation of sensitive information within components of the infrastructure. Particular attention will be paid to protect private (e.g., privacy act) information and information such as identification of law enforcement personnel.

2.6.2 Information Release Circumstances

A CA shall not disclose non-certificate information to any third party unless authorized by this Policy, required by law, government rule or regulation, or order of a court of competent jurisdiction. Any request for release of information shall be authenticated. Information shall only be released where the third party demonstrates possession of a bona fide authorization.

2.7 Intellectual Property Rights

The U.S. Government retains exclusive rights to any products or information developed under or pursuant to this CP, including the public key certificates and private keys.

2.8 Fees

The Treasury PKI/ PMO and PMA reserves the right to impose fees for any or all services provided.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Initial Registration

3.1.1 Types of Names

All CAs shall be able to generate and sign certificates that contain an X.500 Distinguished Name (DN). All certificates issued shall use the DN form. Certificates may additionally assert an alternate name form of the IP address, RFC-822 name, and URL. **The Treasury Office of the CIO is responsible for the assignment and maintenance of DNs.**

For the Treasury employees, the DN will be of the following form:

"CN=userID,OU=bureau,OU=Department of the Treasury,O=U.S. Government,C=US"

The userID is unique across the Treasury directory. It is a non-identifying ID and is 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. There are many individuals in the Department of the Treasury who have sensitive positions. This DN scheme allows all individuals in the Department to take advantage of the OCA while affording these individuals the security they need. The directory can be queried using a subscriber name (as long as access controls are not in place to protect it) 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

3.1.2 Need for Names to be Meaningful

Subject names used in the certificates must identify the person or object to which they are assigned in a meaningful way.

When DNs are used, the userID shall represent the subscriber. For equipment, this may be a model name and serial number, or an application process (e.g., Organization X Mail List or Organization Y Multifunction Interpreter).

3.1.3 Rules for Interpreting Various Name Forms

Rules for interpreting name forms shall be in accordance with the appropriate standard, i.e., X.500 for DN, RFC-822 for Internet e-mail address, and appropriate Internet RFCs for URL and IP.

3.1.4 Uniqueness of Names

Name uniqueness across the OCIO PKI shall be enforced **by the Treasury Office of the CIO**. The userID attribute is used to ensure that no two individuals are assigned the same DN, and therefore the same electronic identity. DNs are guaranteed to be unique throughout the Treasury PKI and must never be reused.

3.1.5 Name Claim Dispute Resolution Procedure

The Treasury PMO shall resolve any name collisions brought to its attention.

3.1.6 Recognition, Authentication and Role of Trademarks

No stipulation.

3.1.7 Method to Prove Possession of Private Key

Since the signature keys will be generated by the subscribers, proof of possession of the private key shall be required. This may be done by the subscriber using its private key to sign a value and providing that value to the CA. The CA shall then validate the signature using the subscriber's public key.

For key management keys if the subscribers generate their own key pairs (which will be the case normally), the CA, RA, or LRA may encrypt the Subscriber's certificate in a confirmation request message. The Subscriber can then decrypt and return the certificate to the CA or RA in a confirmation message.

The Treasury PMO may allow other mechanisms that are at least as secure as those cited here.

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

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

3.1.8 Authentication of Organization Identity

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

3.1.9 Authentication of Individual Identity

A CA, RA, or LRA shall ensure that the applicant's identity information is verified in accordance with the applicable assurance level. The CA shall ensure that the applicant's identity information and public key are properly bound. Additionally, the CA, RA, or LRA shall record the process that was followed for issuance of each certificate. Process information shall depend upon the certificate level of assurance and shall be addressed in the CA CPS. The process documentation and authentication requirements shall include the following depending upon the level of assurance (as set forth below):

- The identity of the person performing the identification;
- A signed declaration by that person that he or she verified the identity of the Subscriber as required by the applicable certificate policy;
- A unique identifying number from the ID of the verifier and, if in-person identity proofing is done, from the ID of the applicant;

- The date and time of the verification;

- A declaration of identity signed by the applicant using a handwritten signature. If in-person identity proofing is done, this shall be performed in the presence of the person performing the identity authentication.

For All Levels: If an Applicant is a system component (e.g., a firewall), the applicant shall be represented by a trusted person already issued a digital certificate by the OCIO PKI. The trusted person will present information sufficient for registration at the level of the certificate being requested, for both himself/herself and the applicant who the trusted person is representing.

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

Assurance Level	Identification Requirements
Level 1	No identification requirement; applicant may apply and receive a certificate by providing his or her e-mail address
Level 2	Identity may be established by comparison with trusted information in a data base, of user-supplied information. Users shall provide a PIN or secret information using the Secure Socket Layer protocol with 128 bit encryption or an alternative approved by the Treasury PMA
Level 3	Identity established by in-person appearance before the Registration Authority. Credentials required are either one Federal Government-issued photo I.D., or two Non-Federal Government I.D.s, one of which shall be a photo I.D. (e.g., Driver's License)
Level 4	Identity established by in-person appearance before the Registration Authority. Credentials required are one Treasury-issued photo I.D., and another photo I.D. (e.g., Driver's License)

3.1.10 Authentication of Component Identities

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

- Equipment identification

- Equipment public key

- **Equipment authorizations and attributes (if any are to be included in the certificate)**

- Contact information to enable the CA, RA, or LRA to communicate with the PKI sponsor when required

The registration information shall be verified to an assurance level commensurate with the certificate assurance level being requested. **The issuing CA will always issue certificates at the same level or lower than its own Assurance Level**. Acceptable methods for performing this authentication and integrity checking include, but are not limited to:

- Verification of digitally signed messages sent from the PKI sponsor (using certificates of equivalent or greater assurance than that being requested).

- In person registration by the PKI sponsor, with the identity of the PKI sponsor confirmed in accordance with the requirements of Section 3.1.9.

3.2 Certificate Renewal, Update, And Routine Re-Key

3.2.1 Certificate Re-key

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

The public key lifetimes given are maximums. A program may always require shorter lifetimes. Signature private keys should be stopped from usage some time before the public key expires. The key management private key can be used any time to decrypt the information. The following public key lifetimes are for Subscribers and RAs; CA key lifetimes are provided in Section 4.7:

Assurance Level	Public Key Certificate Life Times
Level 1	Signature and key management keys re-key every seven years
Level 2	Signature and key management keys re-key every five years
Level 3	Signature and key management keys re-key every three years
Level 4	Signature and key management keys re-key every three years

For the various assurance levels, upon rekey, the subscribers shall be authenticated as listed below:

Assurance Level	Routine Rekey Identification and Authentication Requirements for Subscriber Signature and Encryption Certificates
Level 1	Identity may be established through use of current signature key
Level 2	Identity may be established through use of current signature key, except that identity shall be reestablished through initial registration process at least once every 15 years from the time of initial registration
Level 3	Identity may be established through use of current signature key, except that identity shall be established through initial registration process at least once every nine years from the time of initial registration
Level 4	Identity may be established through use of current signature key, except that identity shall be established through initial registration process at least once every three years from the time of initial registration

3.2.2 Certificate Renewal

Renewing a certificate means creating a new certificate with the same name, key, and other information as the old one, but a new, extended validity period and a new serial number. A certificate shall be renewed only if the public key has not reached the end of its validity period, the associated private key has not been

compromised, and the Subscriber name and attributes are unchanged. The CA may automatically renew a subscriber certificate or using the same rules as those for rekey listed above for the various assurance levels.

3.2.3 Certificate Update

Updating a certificate means creating a new certificate that has the same or a different key, a different serial number, and differs in one or more other fields, from the old certificate. **The old certificate must be not be further rekeyed, updated or renewed.**

If an individual's name changes (e.g., due to marriage), then the same process as the initial registration shall be followed. Otherwise, the rekey rules for the various assurance levels listed above may be used.

3.3 Obtaining A New Certificate After Revocation

In the event of certificate revocation, issuance of a new certificate shall always require that the party go through the initial registration process per Section 3.1 above.

3.4 Revocation Request

Revocation requests must be authenticated (see Section 4.4.1.3). Requests to revoke a certificate may be authenticated using that certificate's associated public key, regardless of whether or not the private key has been compromised.

4. OPERATIONAL REQUIREMENTS

4.1 Certificate Application

The applicant and the OCIO PKI shall perform the following steps when an applicant applies for a certificate:

- The OCIO PKI shall establish, authenticate and record the subscriber identity per Section 3.1;
- The subscriber shall generate a public/private key pair for each certificate required;
- The subscriber shall provide the public key to the OCIO PKI as described in Section 4.1.1 below;
- The OCIO PKI shall verify that the public key forms a functioning key pair with the private key held by the Subscriber as described in Section 3.1.7;

All communications among the OCIO PKI components and the subscriber shall be authenticated and protected from modification using mechanisms commensurate with or stronger than the requirements of the data to be protected by the certificates being issued (e.g., communications supporting the issuance of Level 3 certificates shall be protected using Level 3 or Level 4 certificates). Any electronic transmission of shared secrets shall be protected (e.g., encrypted) using means commensurate with the requirements of the data to be protected by the certificates being issued.

CAs implementing this CP shall certify other CAs (to include cross-certification) only after obtaining written authorization from the Treasury PMA. CAs shall only issue certificates asserting the policies listed in this CP upon receipt of written authorization from the Treasury PMO, and then may only do so within the constraints imposed by the Treasury PMO or its designated representatives.

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

The Treasury PMO shall evaluate the submitted CPS for acceptability. The Treasury PMO may require an initial compliance audit, performed by parties of the Treasury PMO's choosing, to ensure that the applicant CA is prepared to implement all aspects of the submitted CPS, prior to the Treasury PMO authorizing the CA to issue and manage certificates asserting the policies listed in this CP.

4.1.1 Delivery of Subscriber Public Key to Certificate Issuer

Public keys shall be delivered for certificate issuance in a way that binds the applicant's verified identification to the public key. For levels 2 through 4, this binding shall be accomplished using means that are as secure as the security offered by the keys being certified. For example, if cryptography is used, it shall be at least as strong as that employed in certificate issuance. For Level 1 assurance, no trusted delivery mechanism is required. For all assurance levels, the method used for public key delivery shall be set forth in a CPS.

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

4.2 Certificate issuance

Upon receiving a request for a certificate from an applicant, appropriate OCIO PKI component (most likely the LRA) shall perform the following actions:

- verify the identity of the requestor;
- verify the authority of the requestor and the integrity of the information in the certificate request;
- build and sign a certificate, if all certificate requirements have been met (in the case of an RA or LRA, have the CA sign the certificate); and
- make the certificate available to the Subscriber.

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

While the Subscriber may do most of the data entry, it is still the responsibility of the CA, RA, or LRA to verify that the information is correct and accurate. This may be accomplished through a system approach linking trusted databases containing personnel information, other equivalent authenticated mechanisms, or through personal contact with the Subscriber's sponsoring organization. If databases are used to confirm Subscriber information, then these databases shall be protected from unauthorized modification to a level commensurate with the level of assurance of the certificate being sought.

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

4.2.1 Delivery of Subscriber's Private Key to Subscriber

For Assurance Levels 3 and 4, a subscriber's digital signature private key will be generated by the subscriber and will remain within the cryptographic boundary of the cryptographic module. **Anyone who generates a private signing key for a Subscriber shall not retain any copy of the key. Hardware tokens containing CA private signature keys may be backed-up in accordance with security audit requirements defined Section 4.5.1. Private signing keys will not be shared by multiple subscribers in the Treasury PKI**.

In most cases, a subscriber's key management private key will be generated by the subscriber and remain within the cryptographic boundary of the cryptographic module. The subscriber key management private key may be generated by the OCIO PKI and delivered to the subscriber. In that case, the module shall be delivered to the Subscriber. Accountability for the location and state of the module shall be maintained until the Subscriber accepts possession of it. The Subscriber shall acknowledge receipt of the module. Under no circumstances shall anyone other than the Subscriber have knowledge of or control over private signing keys. CA Public Key Delivery to Subscribers

The public key of the Treasury Root CA shall be available for certification trust paths to be created and verified. That key shall appear in the form of a self-signed public key certificate. This self-signed certificate shall be delivered to the subscribers in a manner that is commensurate with the security offered by the public key in the certificate. Acceptable methods for the self-signed certificate delivery include but are not limited to:

- The CA loading the certificate onto tokens delivered to subscribers via secure mechanisms;

- Secure distribution of the certificates through secure out-of-band mechanisms;

- Comparison of certificate hash or fingerprint against the certificate hash or fingerprint made available via authenticated out-of-band sources (note that fingerprint or hash posted in-band along with the certificate are not acceptable as an authentication mechanism); and

- Loading certificates from web sites secured with a currently valid certificate of equal or greater assurance level than the certificate being downloaded.

Systems using Level 4 certificates shall store the level 4 trust root self-signed certificate such that unauthorized alteration or replacement is readily detectable.

4.3 Certificate Acceptance

For level 1, there are no requirements in this area.

For all other levels, the subscriber shall be required to acknowledge his or her obligations with respect to protection of the private key and use of the certificate before being issued the certificate. For levels 3 and 4, the subscriber acknowledgement shall be in the form of a handwritten signature. In the case of non-human components (router, firewalls, etc.), the PKI Sponsor shall perform the functions of the Subscriber.

4.4 Certificate Suspension and Revocation

4.4.1 Revocation

4.4.1.1 Circumstances for Revocation of a Certificate

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

- Identifying information in the certificate become invalid;

- The Subscriber can be shown to have violated, or is suspected of violating, the subscriber obligations as stipulated in this CP and applicable CPS;

- The private key has been or is suspected of having been compromised, or has been lost, stolen, or destroyed in a fashion where there is potential for compromise or loss of control over the use of the private key;

- The subscriber or other authorized party (as defined in the CPS) asks for his/her certificate to be revoked.

Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on the CRL. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.

4.4.1.2 Who Can Request Revocation of a Certificate

A CA may revoke certificates within its domain. A written notice and brief explanation for the revocation shall subsequently be provided to the Subscriber.

An RA can request the revocation of a Subscriber's certificate on behalf of any authorized party as specified in its CPS. The LRA can petition the RA to revoke a Subscriber's certificate.

A subscriber can request the revocation of her own certificate(s).

4.4.1.3 Procedure for Revocation Request

A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed). In particular, if the revocation is being requested for reason of key compromise or suspected fraudulent use, then the revocation request shall always indicate that.

A CA shall authenticate the certificate revocation request and validate the authority of the requester to request the revocation of that certificate.

For PKI implementations using hardware tokens, a Subscriber ceasing its relationship with an organization that sponsored the certificate shall, prior to departure, surrender to the organization (through any accountable mechanism) all cryptographic hardware tokens that were issued by or on behalf of the sponsoring organization.

The token shall be zeroized or destroyed prior to, or immediately upon, surrender in the presence of the Subscriber, or shall be zeroized or destroyed promptly and shall be protected from malicious use prior to zeroization or destruction.

If a Subscriber leaves an organization and the hardware tokens cannot be obtained from the Subscriber, then all Subscriber's certificates associated with the unretrieved tokens shall be immediately revoked. The reason code "key compromise" shall be asserted in this situation.

4.4.1.4 Revocation Request Grace Period

There is no revocation grace period for the subscribers. Subscribers and other authorized parties (as defined in the CPS) shall request revocation of a certificate as soon as they recognize the need for revocation.

The CRL publication requirements for the CA are listed in Section 4.4.3

4.4.2 Suspension

Suspension shall not be used by the OCIO PKI.

4.4.3 Certificate Revocation Lists

4.4.3.1 CRL Issuance Frequency

CRLs shall be issued periodically, even if there are no changes to be made, to ensure timeliness of information. CRLs may be issued more frequently than the issuance frequency described below. The CAs shall remove older CRLs from the repository upon posting the current one.

All CRLs shall populate nextUpdate field. CRLs shall be published not later than the next scheduled update as defined in the nextUpdate field.

The following table provides CRL issuance requirements.

Assurance Level	CRL Issuance Frequency	CRL Issuance (Loss or Compromise of Private Key)
Level 1	Not Required	Within 24 Hours of Notification
Level 2	Every 7 days	Within 24 Hours of Notification
Level 3	At Least Once Each Day	**Within 18 Hours of Notification**
On-Line Level 4	At Least Once Each Day	Within 6 Hours of Notification
Off-Line Level 4	Monthly	Immediately upon Notification

4.4.3.2 CRL Checking Requirements

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

For Class 3 and 4, the relying parties shall obtain the current CRL. A CRL shall be considered current for this CP if the next update field in the CRL is later than the current time.

4.4.4 On-line Revocation / Status Checking Availability

The OCIO PKI shall not support this capability.

4.4.5 Other Forms of Revocation Advertisements Available

No stipulation.

4.4.6 Checking Requirements for Other Forms of Revocation Advertisements

No stipulation.

4.4.7 Special Requirements Related to Key Compromise

In the event of a subscriber private key compromise or loss, a CRL shall be immediately published by the CA.

4.5 Security Audit

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

4.5.1 Types of Events Recorded

All security auditing capabilities of the CA and RA 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. (Note: the table below may be replaced in future releases of this CP with a reference to the Certificate Issuing and Management Components (CIMC) Protection Profile being developed by NIST.) At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- The type of event
- The date and time the event occurred
- A success or failure indicator
- Identity of the entity and/or operator that caused the event.

Message from any source requesting an action by a CA or an RA is an auditable event. The message must include message date and time, source, destination and contents.

Auditable Event	Level 1	Level 2	Level 3	Level 4
SECURITY AUDIT				
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
IDENTIFICATION AND AUTHENTICATION				
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
LOCAL DATA ENTRY				
All security-relevant data that is entered in the system		X	X	X

Auditable Event	Level 1	Level 2	Level 3	Level 4
REMOTE DATA ENTRY				
All security-relevant messages that are received by the system		X	X	X
DATA EXPORT AND OUTPUT				
All successful and unsuccessful requests for confidential and security-relevant information		X	X	X
KEY GENERATION				
Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)	X	X	X	X
PRIVATE KEY LOAD AND STORAGE				
The loading of Component private keys	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
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE				
All changes to the trusted public keys, including additions and deletions	X	X	X	X
SECRET KEY STORAGE				
The manual entry of secret keys used for authentication			X	X
PRIVATE AND SECRET KEY EXPORT				
The export of private and secret keys (keys used for a single session or message are excluded)	X	X	X	X

Auditable Event	Level 1	Level 2	Level 3	Level 4
CERTIFICATE REGISTRATION				
All certificate requests	X	X	X	X
CERTIFICATE REVOCATION				
All certificate revocation requests		X	X	X
CERTIFICATE STATUS CHANGE APPROVAL				
The approval or rejection of a certificate status change request		X	X	X
CA, RA, or LRA CONFIGURATION				
Any security-relevant changes to the configuration of the CA or the RA		X	X	X
ACCOUNT ADMINISTRATION				
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
CERTIFICATE PROFILE MANAGEMENT				
All changes to the certificate profile	X	X	X	X
REVOCATION PROFILE MANAGEMENT				
All changes to the revocation profile		X	X	X
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT				

Auditable Event	Level 1	Level 2	Level 3	Level 4
All changes to the certificate revocation list profile		X	X	X
MISCELLANEOUS				
Installation of the Operating System		X	X	X
Installation of CA,r RA, or LRA		X	X	X
Installing hardware cryptographic modules			X	X
Removing hardware cryptographic modules			X	X
Destruction of cryptographic modules		X	X	X
System Startup		X	X	X
Logon Attempts on CA,r 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
Restoring CA, RA, LRA internal database		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
Shipment of Tokens			X	X
Zeroizing tokens		X	X	X
Rekey of the CA	X	X	X	X
Configuration changes to the CA server RA, or LRA involving:				
Hardware		X	X	X

Auditable Event	Level 1	Level 2	Level 3	Level 4
Software		X	X	X
Operating System		X	X	X
Patches		X	X	X
Security Profiles			X	X
PHYSICAL ACCESS / SITE SECURITY				
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
ANOMALIES				
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

4.5.2 Audit Processing Frequency

Audit logs shall be reviewed in accordance to the table below. All significant events shall be explained in an audit log summary. Such reviews involve verifying that the log has not been tampered with, and then

briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews shall be documented.

Assurance Level	Review Audit Log
Level 1	Only required for cause
Level 2	Only required for cause
Level 3	At least once every two months 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
Level 4	At least once per month 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

4.5.3 Retention Period for Audit Data

Audit logs shall be retained onsite for at least two months as well as being retained in the manner described below. The individual who removes (i.e., rotates or backs up) audit logs from the CA system shall be an official different from the individuals who, in combination, command the CA signature key.

4.5.4 Protection of Audit Data

The audit process shall not be done by or under the control of the individual(s) who command the CA signature key. The CA shall ensure that:

- only authorized people have read access to the logs;
- only authorized people may archive or delete audit logs; and ,
- audit logs are not modified.

The entity performing audit log archive need not have modify access, but procedures must be implemented to protect archived data from deletion or destruction prior to the end of the audit log retention period (note that deletion requires modification access). Audit logs shall be moved to a safe, secure storage location separate from the CA equipment.

In addition, for assurance levels 3 and 4, the audit log shall be stored on Write Once Read Many (WORM) medium, obviating the need for back up and deletion.

4.5.5 Audit Data Backup Procedures

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

4.5.6 Audit Collection System (internal vs. external)

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

4.5.7 Notification to Audit Event-causing Subject

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

4.5.8 Vulnerability Assessments

See section 4.5.2 for audit processing requirements. This processing shall be used to assess the potential vulnerabilities of the system.

4.6 Records Archival

4.6.1 Types of Events Archived

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

At a minimum, the following data shall be recorded for archive in accordance with each assurance:

Data To Be Archived	Level 1	Level 2	Level 3	Level 4
CA accreditation (if applicable)	X	X	X	X
Certification Practice Statement	X	X	X	X
Contractual obligations	X	X	X	X
System and equipment configuration	X	X	X	X
Modifications and updates to system or configuration	X	X	X	X
Certificate requests	X	X	X	X
Revocation requests		X	X	X
Subscriber identity Authentication data as per Section 3.1.9		X	X	X
Documentation of receipt and acceptance of certificates		X	X	X

Data To Be Archived	Level 1	Level 2	Level 3	Level 4
Documentation of receipt of tokens		X	X	X
All certificates issued or published	X	X	X	X
Record of CA Re-key	X	X	X	X
All CRLs issued and/or published		X	X	X
All Audit Logs	X	X	X	X
Other data or applications to verify archive contents		X	X	X
Documentation required by compliance auditors		X	X	X

4.6.2 Retention Period for Archive

The minimum retention period for archive data are identified below. The minimum retention periods are subject to change depending on the outcome of pending legal guidance.

Assurance Level	Retention Period
Level 1	7 Years & 6 Months
Level 2	7 Years & 6 Months
Level 3	10 Years & 6 Months
Level 4	20 Years & 6 Months

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site. Applications required to process the archived data shall also be maintained for the same period as the archived records are kept.

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

4.6.3 Protection of Archive

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

4.6.4 Archive Backup Procedures

No stipulation.

4.6.5 Requirements for Time-stamping Archive Records

No stipulation.

4.6.6 Archive Collection System (internal or external)

The Treasury OCA is archiving its records in accordance with procedures authorized by the National Archives and Records Administration for the Department of the Treasury.

4.6.7 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 CA CPS.

4.7 Key Changeover

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

The table below provides the validity periods of the CA signing keys and corresponding certificates.

Assurance Level	CA (signing key/certificate validity period) (all values are in years)
Level 1	5/10
Level 2	5/10
Level 3	3/6
Level 4	3/6

4.8 Compromise and Disaster Recovery

4.8.1 Computing Resources, Software, and/or Data

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

4.8.2 Private Key Compromise

If a CA cannot issue a CRL prior to the time specified in the nextUpdate field of its currently valid CRL, then the CA certificate shall be revoked and the CA shall be rekeyed. The CA shall be issued new public key certificates by appropriate CA(s). These procedures shall also be used if the CA key is compromised, CA cryptographic module is lost, or CA key is suspected of being compromised.

In addition, if the CA is the Treasury root or the agency root as the relying party trust anchor, the OCIO PKI subscribers who rely on that trust anchor shall be notified using out-of-band means to delete the trust

anchor and to obtain the new trust anchor key in a trusted manner. These means shall be described in the CA CPS.

The CA shall also investigate and report to the Treasury PMO what caused the compromise or loss, and what measures have been taken to preclude recurrence.

4.8.3 Facility Disaster

In the case of a disaster whereby a CA installation is physically damaged and all copies of the CA signature key are destroyed as a result, **revocation of all certificates issued to that CA shall be requested**. The CA installation shall then be completely rebuilt, by reestablishing the CA equipment, generating new private and public keys, being re-certified, and re-issuing all certificates.

In addition, if the CA is the Treasury Root as the relying party trust anchor, the Treasury subscribers who rely on that trust anchor shall be notified using out-of-band means to delete the trust anchor and to obtain the new trust anchor key in a trusted manner. These means shall be described in the Treasury Operational CA CPS.

4.9 CA Termination

In the event of termination of a CA operation, certificates signed by the CA shall be revoked. All certificates issued to the terminating CA shall also be revoked. Prior to CA termination, the CA shall provide archived data to a Treasury PMO approved archival facility.

5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS

5.1 Physical Controls

The CAs shall impose physical security requirements that provide similar levels of protection as those specified below.

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

5.1.1 Site Location and Construction

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

5.1.2 Physical Access

The CA equipment shall always be protected from unauthorized access.

These security mechanisms shall be commensurate with the level of threat in the equipment environment. There are no additional specific requirements for CAs that issue only assurance level 1 certificates.

The physical security requirements pertaining to CAs that issue assurance level 2 certificates are to:

- Ensure no unauthorized access to the hardware is permitted
- Ensure all removable media and paper containing sensitive plain-text information is stored in secure containers

In addition to those requirements, the following requirements shall apply to CAs that issue assurance levels 3 and 4 certificates:

- Be manually or electronically monitored for unauthorized intrusion at all times (Ensure the CA workstation is monitored at all times for unauthorized intrusion or access)
- Ensure an access log is maintained and inspected periodically

Removable cryptographic modules shall be inactivated prior to storage. When not in use, removable cryptographic modules, and activation information used to access or enable cryptographic modules and/or CA equipment shall be placed in secure containers. For assurance levels 3 and 4, the containers shall be GSA approved Class VI security containers. Activation data shall either be memorized, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module.

A security check of the facility housing the CA equipment (operating at the assurance level 2 or higher) shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:

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

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

5.1.3 Electrical Power

A CA (operating at the assurance level 2 or higher) shall have backup power supply capability sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. The directories shall be provided with Uninterrupted Power sufficient for a minimum of six hours operation in the absence of commercial power.

5.1.4 Water Exposures

No stipulation.

5.1.5 Fire Prevention and Protection

No stipulation.

5.1.6 Media Storage

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

5.1.7 Waste Disposal

No stipulation.

5.1.8 Off-site Backup

For the CAs (operating at the assurance level 2 or higher), full system backups, sufficient to recover from system failure, shall be made on a periodic schedule, 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

5.2.1 Trusted Roles

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

A CA shall be configured and operated using the following roles:

1. OCA Administrator – authorized to operate the OCA server and perform system backup and recovery.
2. *RAs and LRAs* authorized to request or approve certificates or certificate revocations, configure profiles and maintain user accounts.
3. *.Auditor* – authorized to view and maintain audit logs.
4. *Operator* – authorized to perform system backup and recovery.
5. *Information Systems Security Officer(ISSO)* – authorized root access to the Treasury Root CA and the Treasury OCA and responsible for a particular component's security.

These roles also create US Treasury RAs and LRAs as directed by the Treasury PKI PMO.

5.2.1.1 The OCA Administrator

The OCA administrator role is responsible for the operation and maintenance of the OCA server this includes:

- Software Back-ups:
  - Operating system
  - Operating system logs
  - Incremental back-ups (Once per day)
  - Full back-ups (Once per seven days)
- Monitors the OCA software application platform and reports services down
- Performs operation and maintenance of the OCA hardware and operating system
- Executes script/routines that manage operating system log creation and deletion on the OCA
- Initiates Change Control procedures for Operating System upgrades and/or patches
- Provides weekly access for Master User at warm backup OCA.

Administrators do not issue certificates to subscribers.

5.2.1.2 RA/LRA

The officer role is responsible for issuing certificates, that is:

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

5.2.1.3 requesting, approving and executing the revocation of certificates

5.2.1.4 Auditor

The auditor role is responsible for:

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

5.2.1.5 Information Systems Security Officer (ISSO)

An ISSO is authorized root access to the Treasury Root CA, OCA and warm backup OCA.

5.2.2 Separation of Roles

Role separation, when required as set forth below, may be enforced either by the CA equipment, or procedurally, or by both means:

Assurance Level	**Role Separation Rules**
Level 1	No stipulation.
Level 2	Individual CA personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume more than one role, however, no one individual shall assume both the Officer and Administrator roles. This may be enforced procedurally. No individual shall be assigned more than one identity.
Level 3	Individual CA personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume more than one role, however, individuals who assume an Officer role may not assume an Administrator or Auditor role. The CA system shall identify and authenticate its users and shall ensure that no user identity can assume both an Administrator and an Officer role. No individual shall be assigned more than one identity.
Level 4	Individual CA personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume only one of the RA, LRA, Administrator, and Auditor roles, but any individual may assume the Operator role. The CA system shall identify and authenticate its users and shall ensure that no user identity can: • Assume both the Administrator and RA/LRA roles • Assume both the Administrator and Auditor roles • Assume both the Auditor and RA/LRA roles. No individual shall have more than one identity.

The Treasury root shall operate at the Level 4 assurance.

5.2.3 Number of Persons Required per Task

Sufficient staff shall be assigned so that the role separation requirements stated above are enforced and the CA can smoothly operate during its operating hours.

5.2.4 Identification and Authentication for Each Role

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

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience, and Security Clearance Requirements

The CA CPS shall identify the individuals that are responsible and accountable for the CA operation.

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

5.3.2 Background Check Procedures

Personnel operating the CAs that issue level 2 or level 3 certificates, shall have a full field Background Investigation using the Standard Form 86, "Questionnaire for National Security Positions".

Personnel operating the CAs that issue level 4 certificates, shall have a Single Scope Background Investigation using the Standard Form 86, "Questionnaire for National Security Positions".

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of a CA, RA or LRA shall receive comprehensive training. Training shall be conducted in the following areas:

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

5.3.4 Retraining Frequency and Requirements

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

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

The Treasury PMO shall take appropriate administrative and disciplinary actions against personnel who have performed actions involving the CA, RA or, LRA repository not authorized in this CP or the CA CPS.

5.3.7 Contracting Personnel Requirements

Contractor personnel employed to perform functions pertaining to a CA, RA, or LRA shall meet applicable requirements set forth in this CP.

5.3.8 Documentation Supplied to Personnel

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

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Requirements for generation of pseudo-random numbers, key pairs and symmetric keys for the CA, RA, LRA and subscribers are listed in Section 6.2.1

6.1.2 Private Key Delivery to Subscriber

A CA shall generate its own key pair and therefore shall not need private key delivery. Subscribers will usually generate their own signature keys and thus will not require delivery; where signature keys are generated by a CA, the key(s) shall be delivered in accordance with the requirements of this CP and the applicable CPS. For encryption keys, delivery of the private key to the Subscriber (or, if the Subscriber generates the encryption key pair, delivery by the Subscriber to the OCIO PKI for key escrow) shall be in accordance with the requirements of this CP and the applicable CPS.

6.1.3 Subscriber Public Key Delivery to Certificate Issuer

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

6.1.4 CA Public Key Delivery to Subscribers

The CAs (e.g., Treasury root and agency root) that form trust anchors for subscribers, shall deliver their public keys to the subscribers in accordance with the requirements of this CP (i.e., Section 4.2.2 CA Public Key Delivery to Subscribers) and in accordance with the applicable CPS.

6.1.5 Key Sizes

All FIPS-approved signature algorithms shall be considered acceptable. If the Treasury PMO determines that the security of a particular algorithm may be compromised, the CAs shall revoke all certificates signed using that algorithm and all certificates that assert the algorithm for the subscribers.

The key size requirements set forth in this section apply to both the CA signing key pair and the subscriber key pair.

Certificates issued for assurance levels 1 through 3, 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 186-1. Certificates issued for assurance level 4 shall use at least 2048 bit RSA, DSA, or DH and SHA 2 of 320 bits.

For assurance levels 1 through 3, Elliptic Curve Digital Signature Algorithm key (ECDSA) and Elliptic Curve Diffie Hellman (ECDH) key prime field (*//p//*) shall be not less that 224, and the Binary Field (*m*)

shall be not less than 233. For assurance level 4, ECDSA key and ECDH key prime field (*//p//*) shall be not less that 384, and the Binary Field (*m*) shall be not less than 409.

Use of SSL or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum triple-DES or equivalent for the symmetric key, and at least 1024 bit RSA or equivalent for the asymmetric keys for assurance levels 1 through 3 and 2048 bit RSA or equivalent for the asymmetric keys for assurance level 4.

6.1.6 Public Key Parameters Generation

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

6.1.7 Parameter Quality Checking

See Section 6.1.6 above.

6.1.8 Hardware/Software Key Generation

The requirements are addressed in Sections 6.1.1 and 6.2.1.

6.1.9 Key Usage (as per X.509 v3 key usage field)

Public keys that are bound into certificates shall be certified for use in signing or encrypting, but not both. The use of a specific key shall be determined by the key usage extension in the X.509 certificate. In particular, subscriber certificates to be used for digital signatures (including authentication) shall set the *digitalSignature* and *nonRepudiation* bits. Certificates to be used for key encryption shall set the *keyAgreement* bit if the algorithm is DH or ECDH and shall set *keyEncipherment* if the algorithm is RSA. CA certificates shall set two key usage bits: *cRLSign* and *keyCertSign*. This restriction is not intended to prohibit use of protocols (like the Secure Sockets Layer) that provide authenticated connections using key management certificates.

6.2 Private Key Protection

6.2.1 Standards for Cryptographic Modules

The relevant standard for cryptographic modules is *Security Requirements for Cryptographic Modules* [latest version of FIPS 140 series]. **For Assurance Level 1 subscriber modules only**, the Treasury PMO may determine that other comparable validation, certification, or verification standards are sufficient. These standards will be published by the Treasury PMO. Cryptographic modules shall be validated to the latest version of the FIPS 140 series level identified in this section, or validated, certified, or verified to requirements published by the Treasury PMO (**Assurance Level 1 subscribers modules only**).

The table below summarizes the minimum requirements for cryptographic modules; higher levels may be used.

Assurance Level	Latest version of FIPS 140 series	Root CA FIPS 140 Level	CA FIPS 140 Level	RA FIPS 140 Level	Subscriber FIPS 140 Level
Level 1	N/A	3 (Hardware)	1	1	N/A
Level 2	Required	3 (Hardware)	2	1	1
Level 3	Required	3 (Hardware)	2 (Hardware)	2 (Hardware)	2 (Hardware)
Level 4	Required	3 (Hardware)	3 (Hardware)	2 (Hardware)	2 (Hardware)

6.2.2 CA Private Key Multi-person Control

The Treasury Root CA, Bureau Root CAs, and all CAs operating at assurance level 3 or higher shall require two or more individuals to activate or back up the CA certificate and CRL signing key(s).

6.2.3 Private Key Escrow

Under no circumstances shall a signature key used to support non-repudiation services be escrowed by a third-party.

The OCIO PKI shall escrow key management keys in accordance with the Key Recovery Policy (KRP) and Key Recovery Practices Statement (KRPS). The KRPS shall be identified in the CPS.

6.2.4 Private Key Backup

6.2.4.1 CA Private Signature Key Backup

A CA private signature keys shall be backed-up under the same multi-person control as the original signature key. Only a single backup copy shall be created. The CPS shall identify the location of the backup.

6.2.4.2 Subscriber Private Signature Key Backup

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

6.2.5 Private Key Archival

Private signature keys shall not be archived.

6.2.6 Private Key Entry into Cryptographic Module

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

Subscriber signature private keys shall be generated by and remain in a cryptographic module.

Subscriber key management keys may be generated outside the cryptographic module and entered in the cryptographic module in accordance with FIPS 140 requirements.

6.2.7 Method of Activating Private Key

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

6.2.8 Methods of Deactivating Private Key

The cryptographic modules that have been activated shall not be left unattended or otherwise available to unauthorized access. After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure, or automatically after a period of inactivity as defined in the applicable CPS. Hardware cryptographic modules shall be removed and stored in accordance with the stipulation of this CP Section 5.1.

6.2.9 Method of Destroying Private Signature Key

Private signature keys shall be destroyed in accordance with FIPS 140 when they are no longer needed, or when the certificates to which they correspond expire or are revoked.

6.3 Practices Regarding Key-Pair Management

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

For information that is encrypted, the subscriber shall use his or her private encryption (confidentiality) key to decrypt the information. If that private key is lost or destroyed, or if the subscriber departs the agency without relinquishing the private key, or acts maliciously, there is no way to decrypt the information. Thus, for business continuity reasons, OCIO PKI shall escrow private keys used for decrypting files and e-mails.

6.3.1 Public Key Archival

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

6.3.2 Usage Periods for the Public and Private Keys

The requirements for the CA keys are described in Section 4.7, Key Changeover.

The requirements for RA, LRA and subscriber keys are described in Section 3.2.1, Certificate Re-key.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The activation data used to unlock private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected. For assurance levels 1 through 3, activation data may be user selected. For assurance level 4, activation data shall either entail the use of biometric data or satisfy the policy enforced at/by the cryptographic module. Activation data shall be generated in conformance with FIPS-112. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

6.4.2 Activation Data Protection

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

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The following computer security functions shall be provided by the operating system for the CA and the RA:

- Require authenticated logins
- Provide Discretionary Access Control
- Provide a security audit capability
- Restrict access control to CA/RA/LRA services and PKI roles
- Enforce separation of duties for PKI roles
- Require identification and authentication of PKI roles and associated identities
- Provide residual information protection for all storage objects
- Require self-test security related operating system services
- Require a trusted path for identification of PKI roles and associated identities
- Enforce process isolation
- Provide self-protection for the above security critical functions of the operating system

CA and RA equipment shall be configured and operated to activate these controls.

The CA and RA application software shall be designed and developed under a development methodology such as MIL-STD-498, the System Security Engineering Capability Maturity Model (SSE CMM), Trusted Software Development Methodology, or the Common Criteria.

Routine self assessments of security controls shall be performed by the entity operating the OCA.

6.5.2 Computer Security Rating

No Stipulation.

6.6 Life-Cycle Technical Controls

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

Hardware and software developed for a CA, RA or LRA shall be developed in a controlled environment, and the development process shall be defined and documented

All hardware and software shall be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the final physical location

The CA hardware and software shall be dedicated to performing the CA. There shall be no other applications, hardware devices, network connections, or component software, which are not part of the CA operation

Proper care shall be taken to prevent malicious software from being loaded onto the CA/RA/LRA equipment. Only applications required to perform the operation of the CA shall be obtained from sources authorized by local policy. RA/LRA hardware and software shall be scanned for malicious code on first use and periodically afterward

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

6.6.1 Security Management Controls

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

6.6.2 Life Cycle Security Ratings

No stipulation.

6.7 Network Security Controls

CA servers and workstations may not be connected to or accessible from, a non-Treasury network. CA servers and workstations may be attached to a Treasury local area network (LAN) or wide area network (WAN), if protected by a dedicated firewall that is located between the LAN/WAN and the CA servers/workstations. An acceptable firewall will consist of a screening router, dual-homed host, or other device, that can control access at both the network and transport protocol layers. This firewall must be configured to only allow a minimal set of inbound and outbound services required for CA operation. **The CA servers and workstations must be monitored at all times for unauthorized intrusion or access**. Unused network ports and services shall be turned off. Any network software and user accounts present shall be necessary to the functioning of the CA.

6.8 Cryptographic Module Engineering Controls

Requirements for cryptographic modules are as stated above in Section 6.2

7. CERTIFICATE AND CRL PROFILES

7.1 Certificate Profile

7.1.1 Version Numbers

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

7.1.2 Certificate Extensions

Rules for the inclusion, assignment of value, and processing of extensions are defined in profiles. Certificate extensions used by the CAs shall conform to the Federal certificate profile established by NIST. These profiles are written to prescribe an appropriate amount of control over an infrastructure, yet be flexible enough to meet the needs of the various CAs and communities. All certificates shall use *Federal PKI Version 1 Technical Specifications: Part E – X.509 Certificate and CRL Extensions Profile* [FPKI-E]. Whenever private extensions are used, they shall be identified in a CPS. Critical private extensions shall be used only if necessary for security reasons.

7.1.3 Algorithm Object Identifiers

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

id-dsa-with-sha1	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3}
sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
ecdsa-with-SHA1	{iso(1) member-body(2) us(840) ansi-x9-62 (10045) signatures (4) 1 }

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

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

7.1.4 Name Forms

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

7.1.5 Name Constraints

Assurance levels 3 and 4 CAs shall use the name constraints extension shall be populated and processed as described in [FPKI-E].

7.1.6 Certificate Policy Object Identifier

Certificates issued under this CP shall assert the OID appropriate to the level of assurance with which it was issued. A certificate issued under level "n" shall assert all the assurance levels up to and including level "n". Thus, a assurance level 4 certificate shall assert all four OIDs. Similarly, a certificate for assurance level 2, shall assert the OIDs for assurance levels 1 and 2.

7.1.7 Usage of Policy Constraints extension

The CAs shall cross certify other domains by inhibiting policy mapping. The FBCA shall be certified by using the value of skipCerts = 1 for the inhibitPolicyMapping field in the policyConstraints extension.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued under this CP shall not contain policy qualifiers.

7.1.9 Processing Semantics for Critical Certificate Policy Extension

Processing semantics for the critical certificate policy extension used shall conform to X.509 2000 version.

7.2 CRL Profile

7.2.1 Version Number

The CAs shall issue X.509 version two (2) CRLs.

7.2.2 CRL and CRL Entry Extensions

Detailed CRL profiles addressing the use of each extension shall conform to [FPKI-E].

8. SPECIFICATION ADMINISTRATION

8.1 Specification Change Procedures

The Treasury PMO shall review this CP at least once every year. The Treasury PMO shall maintain and publish a Certificate Policy Plan that describes anticipated changes to this CP. Errors, updates, or suggested changes to this CP shall be communicated to every cross-certified domain, including FBCA and Subscriber. Such communication shall include a description of the change, a change justification, and contact information for the person requesting the change.

All policy changes under consideration by the Treasury PMO shall be disseminated to interested parties. All interested parties may provide their comments to the Treasury PMO in a manner to be stipulated in the CA CPS.

8.2 Publication and Notification Policies

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

8.3 CPS Approval Procedures

The CA CPS shall be published in a separate document and shall be approved by the Treasury PMO. Domains desiring certification by the OCIO PKI shall submit their CPs and CPSs to the Treasury PMO. The Treasury PMO shall make the determination if and what assurance levels the certificate(s) to the CA(s) in the other domain are issued. This decision shall be based solely on the Treasury PMO's determination of the assurance level equivalency between the OCIO PKI and the other domain's CP and CPS.

8.4 Waivers

Normally, the Treasury PMO shall decide that variation in CA/RA practice is acceptable under this CP, or the CA/RA shall request a permanent change to this CP. Policy waivers may be granted by the Treasury PMO to meet urgent, unforeseen operational requirements (such as those associated with ongoing law-enforcement and financial mission). When a waiver is granted, the Treasury PMO shall post the waiver on a web site accessible by relying parties, and shall either initiate a permanent change to the policy, or shall place a specific time limit, not to exceed one year, on the waiver.

9. BIBLIOGRAPHY

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

ABADSG — Digital Signature Guidelines, 1996-08-01. http://www.abanet.org/scitech/ec/isc/dsgfree.html.

FIPS 112 — Password Usage, 1985-05-30 http://csrs.nist.gov/fips/

FIPS 140-1 — Security Requirements for Cryptographic Modules, 1994-01 http://csrs.nist.gov/fips/fips1401.htm

FIPS 186-1 — Digital Signature Standard, 1994-05-19 http://csrs.nist.gov/fips/fips186.pdf

FOIACT — 5 U.S.C. 552, Freedom of Information Act. Http://www4.law.cornell.edu/uscode/5/552.html

FPKI-E — Federal PKI Version 1 Technical Specifications: Part E-X.509 Certificate and CRL Extensions Profile, 7 July 1997 http://csrs.nist.gov/pki/FPKI7-10.DOC

ISO9594-8 — Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, 1997. ftp://ftp.bull.com/pub/OSIdirectory/ITU/97x509final.doc

ITMRA — 40 U.S.C. 1452, Information Technology Management Reform Act of 1996. Http://www4.law.cornell.edu/uscode/40/1452.html

NAG69C — Information System Security Policy and Certification Practice Statement for Certification Authorities, rev C, November 1999.

NSD42 — National Policy for the Security of National Security Telecom and Information Systems, 5 Jul 1990. Http://snyside.sunnyside.com/cpsr/privacy/computer_security/nsd_42.txt (redacted version)

NS4005 — NSTISSI 4005, Safeguarding COMSEC Facilities and Material, August 1997.

NS4009 — NSTISSI 4009, National Information Systems Security Glossary, January 1999.

PKCS#12 — Personal Information Exchange Syntax Standard, April 1997. Http://www.rsa.com/rsalabs/pubs/PKCS/html/pkcs-12.html

RFC 2510 — Certificate Management Protocol, Adams and Farrell, March 1999.

RFC 2527 — Certificate Policy and Certificate Practices Framework, Chokhani and Ford, March 1999.

TDP71-10 — Treasury Directive???????

Security Requirements for Certificate Issuing and Management Components, 3 November 1999, Draft

Digital Signatures, W. Ford

United States Department of Defense X.509 Certificate Policy, Version 5.0, 13 December

1999

10. ACRONYMS AND ABBREVIATIONS

CA	Certification Authority
CIO	Chief Information Officer
COMSEC	Communications Security
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSOR	Computer Security Object Registry
DH	Diffie Hellman
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ERC	Enhanced Reliability Check
FAR	Federal Acquisition Regulations
FBCA	Federal Bridge Certification Authority
FED-STD	Federal Standard
FIPS PUB	(US) Federal Information Processing Standard Publication
FPKI	Federal Public Key Infrastructure
FPKI-E	Federal PKI Version 1 Technical Specifications: Part E – X.509 Certificate and CRL Extensions Profile
GPEA	Government Paperwork Elimination Act of 1998
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization

ISSO	Information Systems Security Officer
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunications Sector
ITU-TSS	International Telecommunications Union – Telecommunications System Sector
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OCIO	Office of the Chief Information Officer
OID	Object Identifier
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SHA-1	Secure Hash Algorithm, Version 1
S/MIME	Secure Multipurpose Internet Mail Extension
SSL	Secure Sockets Layer
TSDM	Trusted Software Development Methodology
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
U.S.C.	United States Code
WWW	World Wide Web

Signature Page

_____

Chair, Treasury PMO

_____

Chair, Treasury, PMO