



United States Postal Service Certification Practice Statement Version 1

Handbook AS-600

February 2001
Transmittal Letter

A. Explanation. Handbook AS-600, *United States Postal Service Certification Practice Statement, Version 1*, is published and maintained by the eCommerce office. This certification practice statement (CPS) describes the practices the Postal Service certification authority (CA) uses to issue and manage public key certificates and maintain an operational certificate-based public key infrastructure. This CPS also describes the terms and conditions of the various services offered to subscribers. Specifically, this CPS sets forth rules governing the following:

1. The Postal Service acting as the certification authority issuing certificates under this CPS.
2. The subscribers, relying parties, registration authorities, repository service providers and other organizations authorized to participate in the public key infrastructure defined by this CPS and the obligations of each.
3. The categories of electronic communication specified as suitable applications for certificates issued in accordance with this CPS.

The Postal Service public key infrastructure will evolve in phases. Version 1 of the *United States Postal Service Certification Practice Statement* pertains to phase 1 production. Where appropriate, this version will highlight functions that are planned for future evolutionary phases.

B. Lifecycle Management. The Postal Service certification authority will use all reasonable efforts to follow the practices set forth in this handbook for the lifecycle management of certificates issued under this CPS.

C. Publicly Available Certification Practice Statement. The Postal Service makes this CPS publicly available on the Internet (<http://www.usps.com/cps>). This gives users access to enough information to make their own decision about applying for, accepting, using, and relying upon any certificate issued under this CPS.

D. Responsibilities. It is the responsibility of all parties involved in a transaction involving a certificate issued under this CPS to read this CPS and to understand the practices established for the lifecycle management of certificates issued by the Postal Service certification authority. Any use or reliance upon a certificate signifies understanding and acceptance of this CPS and all related policies and agreements.

- E. General Purpose Certification Authority.** The Postal Service intends for the Postal Service CA to be a general-purpose certification authority providing the public key infrastructure foundation for a wide range of business purposes and applications. As such, business-specific and application-specific practices are not included in this CPS. Other documents, such as a certificate policy or service level agreement, will dictate the specific range of practices provided to users in the context of an approved application for which the Postal Service certification authority issues certificates.
- F. Distribution.** This handbook is only published online via the Postal Service Internet (<http://www.usps.com/cps>). All versions of Handbook AS-600 will be archived and available online.
- G. Comments.** Submit questions, comments, or suggestions regarding this handbook in writing to:
- CERTIFICATION AUTHORITY MANAGER
eCOMMERCE OFFICE
US POSTAL SERVICE
475 L'ENFANT PLAZA SW
WASHINGTON DC 20260-6201
- H. Effective Date.** This handbook is effective immediately.



Robert G. Krause
Vice President
eCommerce

Update Notice

Handbook AS-600 United States Postal Service Certification Practice Statement Version 1

We updated this handbook as follows:

- Section 1.2, Policy Identification — Changed CPS object identifier from 2.16.840.113901.101 to 2.16.840.1.11390.101.

July 27, 2001

Contents

1	Introduction	1
1.1	Overview	1
1.2	Policy Identification	1
1.3	Community and Applicability	1
1.3.1	Certification Authority	2
1.3.2	Registration Authority	2
1.3.3	Repositories	2
1.3.4	End Entity, Subscriber, or Certificate Holder	2
1.3.5	Relying Parties	3
1.3.6	Policy Authority	3
1.3.7	Applicability and Applications	3
1.4	Contact Details	4
1.4.1	Specification Administration Organization	4
1.4.2	Contact Person	4
2	General Provisions	5
2.1	Obligations	5
2.1.1	Postal Service Certification Authority Obligations	5
2.1.2	Registration Authority Obligations	6
2.1.3	Repository Obligations	6
2.1.4	Subscriber Obligations	6
2.1.5	Relying Party Obligations	7
2.1.6	Policy Authority Obligations	7
2.2	Liability	8
2.2.1	Disclaimer	8
2.2.2	Loss Limitation	8
2.2.3	Registration Authority Liability	8
2.3	Financial Responsibility	9
2.3.1	Indemnification by Relying Parties and Subscribers	9
2.3.2	Fiduciary Relationships	9
2.4	Interpretation and Enforcement	9
2.4.1	Governing Law	9
2.4.2	Jurisdiction	9
2.4.3	Severability, Survival, Merger, Notice	9
2.4.4	Dispute Resolution Procedures	10
2.5	Fees	10

2.6	Publication and Repository	10
2.6.1	Publication of Certification Authority Information	10
2.6.2	Frequency of Publication	11
2.6.3	Access Controls	11
2.6.4	Repositories	11
2.7	Compliance Audit	12
2.7.1	Frequency of Certification Authority Compliance Review	12
2.7.2	Identity and Qualifications of Reviewer	12
2.7.3	Auditor's Relationship to Audited Party	12
2.7.4	Scope of Audit	12
2.7.5	Actions Taken as a Result of Deficiency	13
2.7.6	Communication of Results	13
2.8	Confidentiality	14
2.8.1	Types of Information to Be Kept Confidential	14
2.8.2	Types of Information Not Considered Confidential	14
2.8.3	Disclosure of Certificate Revocation and Suspension Information	14
2.8.4	Release to Law Enforcement Officials	15
2.8.5	Release as Part of Civil Discovery	15
2.8.6	Disclosure upon Owner's Request	15
2.8.7	Other Information Release Circumstances	15
2.9	Intellectual Property Rights	15
3	Identification and Authentication	17
3.1	Initial Registration	17
3.1.1	Types of Names	17
3.1.2	Name Meanings	17
3.1.3	Rules for Interpreting Various Name Forms	17
3.1.4	Name Uniqueness	17
3.1.5	Name Claim Dispute Resolution Procedures	17
3.1.6	Recognition, Authentication, and Role of Trademarks	18
3.1.7	Verification of Possession of Private Key	18
3.1.8	Authentication of Sponsoring Organization Identity	18
3.1.9	Authentication of Individual Identity (No Affiliation)	19
3.1.10	Authentication of Individual (Affiliated Certificate)	19
3.2	Routine Rekey	20
3.3	Rekey After Revocation	20
3.4	Revocation Request	20

4	Operational Requirements	21
4.1	Certificate Application	21
4.2	Certificate Issuance	21
4.3	Certificate Acceptance	22
4.4	Certificate Suspension and Revocation	22
4.4.1	Who Can Request Revocation	22
4.4.2	Circumstances for Revocation	22
4.4.3	Procedure for Revocation Request	23
4.4.4	Revocation Request Grace Period	23
4.4.5	Circumstances for Suspension	23
4.4.6	Who Can Request Suspension	23
4.4.7	Procedure for Suspension Request	23
4.4.8	Limits on Suspension Period	24
4.4.9	Certificate Revocation List Issuance Frequency	24
4.4.10	Online Revocation and Status Checking Availability	24
4.4.11	Certificate Revocation List Checking Requirements	24
4.4.12	Online Revocation and Status Checking Availability	24
4.4.13	Online Revocation Checking Requirements	24
4.4.14	Other Forms of Revocation Advertisements Available	25
4.4.15	Checking Requirements for Other Forms of Revocation Advertisements	25
4.4.16	Special Requirements Regarding Key Compromise	25
4.5	Computer Security Audit Procedures	25
4.5.1	Types of Events Recorded	25
4.5.2	Frequency of Audit Log Processing	26
4.5.3	Period for which Audit Logs are Kept	26
4.5.4	Protection of Audit Logs	26
4.5.5	Audit Log Backup Procedures	27
4.5.6	Audit Collection System	27
4.5.7	Notification of Audit Subjects	27
4.5.8	Vulnerability Assessments	27
4.6	Records Archival	28
4.6.1	Types of Events Recorded	28
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 of Records	28
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
4.7.1	Root Public Key	29

4.7.2	Changeover Period	29
4.8	Compromise and Disaster Recovery	29
4.8.1	Disaster Recovery Plan	29
4.8.2	Key Compromise Plan	29
4.9	Certification Authority Cessation of Services	30
5	Physical, Procedural, and Personnel Security Controls	31
5.1	Physical Security Controls	31
5.2	Procedural Controls	31
5.2.1	Trusted Roles	31
5.2.2	Number of Persons Required Per Task	32
5.2.3	Identification and Authentication for Each Role	32
5.3	Personnel Controls	32
5.3.1	Background and Qualifications	32
5.3.2	Background Investigation	32
5.3.3	Training Requirements	32
5.3.4	Retraining Frequency and Requirements	32
5.3.5	Sanctions for Unauthorized Actions	33
5.3.6	Contracting Personnel Requirements	33
5.3.7	Documentation Supplied to Personnel	33
6	Technical Security Controls	35
6.1	Key Pair Generation and Installation	35
6.1.1	Key Pair Generation	35
6.1.2	Private Key Delivery to Entity	35
6.1.3	Subscriber Public Key Delivery to Certification Authority	35
6.1.4	Certification Authority Public Key Delivery to Users	35
6.1.5	Key Sizes	36
6.1.6	Key Usage Purposes	36
6.2	Private Key Protection	36
6.2.1	Standards for Cryptographic Module	36
6.2.2	Private Key (n out of m) Multi-Person Control	36
6.2.3	Private Key Escrow	36
6.2.4	Private Key Backup	36
6.2.5	Private Key Archival	36
6.2.6	Private Key Entry into Cryptographic Module	36
6.2.7	Method of Activating Private Key	36
6.2.8	Method of Deactivating Private Key	37
6.2.9	Method of Destroying Private Key	37

Contents

6.3 Other Aspects of Key Pair Management	37
6.3.1 Public Key Certificate Archival	37
6.3.2 Usage Periods for the Public and Private Keys (Key Replacement)	37
6.4 Activation Data	37
6.4.1 Activation Data Generation and Installation	37
6.4.2 Activation Data Protection	37
6.4.3 Other Aspects of Activation Data	38
6.5 Computer Security Controls	38
6.6 Lifecycle Technical Controls	38
6.7 Network Security Controls	38
6.8 Cryptographic Module Engineering Controls	38
7 Certificate and Certificate Revocation List Policies	39
8 Certificate Policy Administration	41
8.1 Certificate Policy Change Procedures	41
8.1.1 Changes Not Requiring Notice	41
8.1.2 Changes Requiring Notice	41
8.2 Publication and Notification Procedures	41
8.3 Certificate Policy Approval Procedures	41
9 Acronyms and Abbreviations	43
10 Glossary	45

1 Introduction

1.1 Overview

A certification practice statement (CPS) is defined by the Internet Engineering Task Force Request for Comment (RFC) 2527, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework and by the American Bar Association Digital Signature Guidelines as “a statement of the practices which a certification authority employs in issuing certificates.” The contents of this CPS follow the framework and recommended elements provided in RFC 2527.

This CPS is incorporated by reference into all contracts between the Postal Service CA and its subscribers and is applicable to all entities with relationships with the Postal Service CA, including subscribers, relying parties, registration authorities, and repository service providers. Other documents, such as a certificate policy or a service level agreement, will dictate the specific range of practices provided to users in the context of an approved application for which the Postal Service CA issues certificates.

The Postal Service CPS is subject to change in accordance with chapter 8 (Certificate Policy Administration) of this handbook.

1.2 Policy Identification

This CPS, Handbook AS-600, is called the *United States Postal Service Certification Practice Statement*. The uniform resource locator or Internet address for this CPS is <http://www.usps.com/cps>. The object identifier for this CPS is 2.16.840.1.11390.101.

1.3 Community and Applicability

This CPS imposes a legal obligation on each of the authorized participants in the Postal Service public key infrastructure community. Authorized participants include the following:

- a. Postal Service CA.
- b. Authorized registration authorities as described in section 1.3.2 (Registration Authority).

- c. Authorized repositories described in section 1.3.3 (Repositories).
- d. Authorized subscribers described in section 1.3.4 (End Entity, Subscriber, or Certificate Holder).
- e. Qualified relying parties described in section 1.3.5 (Relying Parties).

Each participant is restricted in their use of certificates issued in accordance with this CPS to the categories of applications described in section 1.3.7 (Applicability and Applications).

1.3.1 **Certification Authority**

The Postal Service certification authority (CA) is the only CA authorized to issue certificates in accordance with the procedures and policies within this CPS. Cross-certification with other CAs is being considered for the future, however it is not covered by this CPS. For the lifecycle management of certificates that reference this CPS, the Postal Service CA is bound to the terms and conditions described in this handbook.

1.3.2 **Registration Authority**

On behalf of a CA, a registration authority (RA) authenticates or verifies the identity of the subscriber. This policy imposes a legal obligation on all authorized agents that perform services for the Postal Service CA related to the RA function for certificates issued by the Postal Service CA under this CPS.

1.3.3 **Repositories**

This policy imposes a legal obligation on any Postal Service–operated repository or contracted repository service provider that operates and manages a repository on behalf of the Postal Service.

1.3.4 **End Entity, Subscriber, or Certificate Holder**

In this handbook, the term *subscriber* refers to end entities, subscribers, and certificate holders. The subscriber is the subject named or identified in a certificate issued by the Postal Service CA. The subscriber holds a private key that corresponds to the public key listed in that certificate. For the purposes of this CPS, the Postal Service CA may issue certificates to the following types of approved subscribers:

- a. Registration authorities.
- b. Affiliated individuals.
- c. Non-affiliated individuals.
- d. Organizations that qualify.

This policy imposes a legal obligation on each certificate applicant and, upon receipt of a digital certificate, the subscriber. Ensuring compliance with applicable import and export laws is the responsibility of the subscriber of the digital certificate and not the Postal Service.

1.3.5 Relying Parties

For each of the list items in section 1.3.4 (End Entity, Subscriber, or Certificate Holder), the relying party relies upon the binding between the subscriber's name and the associated public key. For the purposes of this CPS, a *relying party* is any entity who relies upon a certificate that is issued by the Postal Service and that is used in a legal manner consistent with this CPS and all related policies and agreements. A relying party is any entity that uses another's certificate for any, all, or a combination of the following reasons:

- a. To verify the integrity of a digitally signed message.
- b. To identify the creator of a message.
- c. To establish confidential communications with the certificate holder.

1.3.6 Policy Authority

The Postal Service eCommerce office (or its successor organization) serves as the policy authority and is responsible for organizing and administering this CPS. This policy is subject to change in accordance with the conditions established in chapter 8 (Certificate Policy Administration) of this CPS.

1.3.7 Applicability and Applications

This certification practice statement applies to all certificates issued by the Postal Service certification authority. The practices described in this CPS apply to the issuance and use of certificates and certificate status information for users within the Postal Service CA domain.

The use of certificates, as described, will be at the discretion of each subscriber and relying party, except to the extent specifically prohibited by the Postal Service CPS, any affiliated certificate policy (CP), or the issued certificate.

1.3.7.1 Suitable Applications

The Postal Service CA can issue certificates in support of a range of certificate policies and applications. Each relying party and subscriber is solely responsible for reading, accepting, and upholding the terms of this CPS and every certificate policy referenced in the issued certificate. The sensitivity of the information processed or protected using a certificate issued by the Postal Service will vary significantly. For this reason, relying parties and subscribers are solely responsible for determining the suitability of conducting a transaction using a certificate issued by the Postal Service CA. Each relying party and subscriber does an evaluation to determine whether an application is suitable. This CPS does not apply to that evaluation.

1.3.7.2 Approved Applications

[Reserved]

1.3.7.3 Prohibited Applications

[Reserved]

1.4 Contact Details

1.4.1 Specification Administration Organization

The Postal Service eCommerce office (or its successor organization) administers this Postal Service certification practice statement.

1.4.2 Contact Person

The Postal Service developed this CPS. Submit questions about Handbook AS-600 in writing to:

CERTIFICATION AUTHORITY MANAGER
eCOMMERCE OFFICE
US POSTAL SERVICE
475 L'ENFANT PLAZA SW
WASHINGTON DC 20260-6201

2 General Provisions

2.1 Obligations

This chapter provides a general description of the roles and responsibilities of the Postal Service CA, subscribers, and relying parties. Additional obligations may be set forth in Postal Service subscriber agreements, service level agreements, affiliated certificate policies, and other agreements and contracts.

2.1.1 Postal Service Certification Authority Obligations

The Postal Service CA is responsible for policies governing the issuance and management of certificates, including the application and enrollment process, the identification and authentication process, the actual certificate manufacturing process, publication of the certificate, suspension and revocation of the certificate, and renewal of the certificate. The CA services, operations, and infrastructure for certificates are performed in accordance with the requirements of this CPS, as well as applicable regulations of the Postal Service.

2.1.1.1 Terms of Issuance

When a certificate references this CPS, the following conditions apply to all subscribers and all relying parties that reasonably and in good faith rely on the information contained in the certificate during its operational period:

- a. The Postal Service CA has complied with the requirements of this CPS and its applicable certificate policies when authenticating the subscriber and issuing the certificate.
- b. Information provided by the subscriber in the certificate application for inclusion in the certificate has been accurately transcribed to the certificate.
- c. The Postal Service CA has taken reasonable steps to verify information in the certificate, unless otherwise noted in this CPS. There are no misrepresentations of fact in the certificate known to the Postal Service CA.

2.1.2 **Registration Authority Obligations**

The RA must verify the accuracy and authenticity of the information a subscriber provides when applying for a certificate. The RA performing this function on behalf of the Postal Service CA must conform to the stipulations of the CPS and any other relevant policy and agreement. Failure to comply in this manner may result in loss of office, loss of associate privileges, and legal sanctions. The RA may use various Postal Service departments, as agents, to verify subscriber-provided data by comparing it with information in corporate employee and contractor databases. When the RA is not an affiliate of the Postal Service, the Postal Service is not under any circumstances liable for the RA's actions or omissions, except as expressly set out in this CPS.

2.1.3 **Repository Obligations**

The Postal Service certification authority maintains a repository of certificates it issues and, optionally, a certificate revocation list for the certificates it revokes.

The Postal Service CA may delegate a repository service provider (RSP) to perform this service, if the RSP conforms to the stipulations of this CPS. *If an RSP is used, then the Postal Service is under no circumstances liable for the RSP's actions or omissions, except as expressly set out in this CPS.*

2.1.4 **Subscriber Obligations**

In all cases, the Postal Service CA requires the subscriber to enter into an enforceable, contractual, or other legal commitment obligating the subscriber to:

- a. Generate a key pair using a trustworthy system, and take reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key.
- b. Implement procedures to preclude key reuse among different roles or across multiple certificates.
- c. Abstain from using their private key for signing purposes until after the public key certificate is formally accepted.
- d. Provide accurate information to the Postal Service CA or to their authorized agent as part of the certificate application process.
- e. Acknowledge that accepting the certificate means the subscriber is certifying that all information and representations made by the subscriber in the certificate are accurate.
- f. Use the certificate exclusively for authorized and legal purposes, consistent with this CPS and in accordance with all applicable certificate policies.
- g. Instruct the Postal Service CA to revoke the certificate promptly upon any actual or suspected loss, disclosure, or other compromise of the subscriber's private key.
- h. Ensure compliance with applicable import and export laws.

- i. Abide by all the terms, conditions, and restrictions levied upon their private keys and certificates.
- j. Notify the Postal Service CA immediately of any change to the information appearing in the subscriber's certificate that occurs during the certificate's validity period.
- k. Accept the Postal Service CA root certificate and applicable Postal Service subordinate root certificates that are needed to facilitate certificate path construction of the subscriber's certificate.

Failure to meet these obligations may result in certificate revocation and the forfeiture of all claims made by the subscriber against the Postal Service in the event of a dispute arising from the failure of the subscriber to meet these obligations. In addition, the subscriber may be liable to the Postal Service CA for any loss or damage that the Postal Service CA suffers as a result.

2.1.5 Relying Party Obligations

A relying party may rely on a certificate that references this CPS only if the certificate was used and relied upon for lawful purposes and under circumstances where the following occurs:

- a. The reliance was reasonable and in good faith in light of all the circumstances known to the relying party at the time of reliance.
- b. The purpose for which the certificate was used was appropriate under this CPS.
- c. The certificate was used exclusively in connection with applicable, approved applications.
- d. The certificate is being used within its operational period.
- e. The relying party checked the status of the certificate prior to reliance, or a check of the certificate's status would have indicated that the certificate was valid.

Failure to meet these obligations results in the forfeiture of any claim against the Postal Service in the event of a dispute and may jeopardize any claim against the subject of the relied upon certificate. In addition, the relying party may be liable to the Postal Service CA for any loss or damage that the Postal Service suffers as a result.

2.1.6 Policy Authority Obligations

The Postal Service eCommerce program management office (or its successor organization) must maintain the accuracy of this document and process changes in accordance with chapter 8 (Certificate Policy Administration) of this CPS.

2.2 Liability

2.2.1 Disclaimer

The Postal Service is not liable for any loss:

- a. Of CA or RA service due to war, natural disasters, or other uncontrollable forces.
- b. Incurred between the time a certificate is revoked and the next scheduled issuance of a certificate revocation list.
- c. Due to unauthorized use of certificates issued by the Postal Service CA, and use of certificates beyond the prescribed use defined by the certificate policy under which it was issued and this CPS.
- d. Caused by fraudulent or negligent use of certificates or certificate revocation lists issued by the Postal Service CA.
- e. Due to disclosure of information contained within certificates and revocation lists.
- f. Of profits, data, or other indirect consequential or punitive damages arising from or in connection with its services.

The Postal Service certification authority has no liability for indirect, special, incidental or consequential damages, or for any loss of profits, loss of data, or other indirect consequential or punitive damages arising from or in connection with its services. Except as expressly provided in this CPS, the Postal Service CA disclaims all other warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of the accuracy of information provided.

2.2.2 Loss Limitation

The Postal Service disclaims any liability that may arise from the use of the Postal Service CA.

2.2.3 Registration Authority Liability

The RA is solely responsible for any claims of loss related to the non-performance of the RA duties in accordance with applicable sections of this CPS, all affiliated certificate policies, applicable service level agreements, and other agreements and contracts. The Postal Service CA has no liability for indirect, special, incidental or consequential damages, or for any loss of profits, loss of data, or other indirect, consequential or punitive damages arising from or in connection with the RA.

2.3 Financial Responsibility

2.3.1 Indemnification by Relying Parties and Subscribers

The relying parties and subscribers must indemnify the Postal Service CA, holding it harmless in accordance with section 2.2.2 (Loss Limitation) if the loss incurred from the transaction is found to be at the fault of the Postal Service CA. The Postal Service CA will not be responsible for loss due to the failure of the subscribers and relying parties to fulfill their obligations under this CPS as described in sections 2.1.4 (Subscriber Obligations) and 2.1.5 (Relying Party Obligations). In particular, the Postal Service CA will not be responsible for loss due to the compromise of the subscriber's private key and for loss due to the inaccuracy of information provided by the subscriber.

Where applicable, the Postal Service CA may seek compensation from a subscriber or relying party if it can be shown that negligent or wrongful acts of a subscriber or relying party have caused the Postal Service CA loss, either financially or in reputation.

2.3.2 Fiduciary Relationships

Issuance of certificates in accordance with this certification practice statement does not make the Postal Service certification authority or any authorized registration authorities, an agent, fiduciary, broker, trustee, or other representative of subscribers or relying parties.

This CPS does not create a partnership or a relationship of principal and agent between the Postal Service CA and any subscriber or between the Postal Service CA and any relying party.

2.4 Interpretation and Enforcement

2.4.1 Governing Law

The enforceability, construction, interpretation, and validity of this CPS is governed by the federal laws of the United States, and if no such law is applicable, the laws of the State of New York.

2.4.2 Jurisdiction

The federal courts of the District of Columbia will have jurisdiction over any disputes arising in connection with this certification practice statement.

2.4.3 Severability, Survival, Merger, Notice

Entire Agreement. This agreement, applicable Postal Service regulations, and subscriber agreements constitute the entire agreement between the parties with respect to the subject matter hereof and merges all prior and contemporaneous communications. It must not be modified except by a

written agreement dated subsequent to the date of this CPS and signed on behalf of the Postal Service by its duly authorized representatives.

Construction. If for any reason a court of competent jurisdiction finds any provision of this CPS, or portion thereof, to be unenforceable, that provision of the CPS will be enforced to the maximum extent permissible so as to effect its intent, and the remainder of this CPS will continue in full force and effect. Failure by the Postal Service to enforce any provision of this CPS will not be deemed a waiver of future enforcement of that or any other provision.

Notices. All notices and requests in connection with this CPS will be deemed given as of the day they are received either by messenger, nationally recognized delivery service, or in the U.S. mail, postage prepaid, certified or registered, return receipt requested, and addressed as follows:

CERTIFICATION AUTHORITY MANAGER
eCOMMERCE OFFICE
US POSTAL SERVICE
475 L'ENFANT PLAZA SW
WASHINGTON DC 20260-6201

2.4.4 **Dispute Resolution Procedures**

[No stipulation.]

2.5 Fees

The Postal Service certification authority does not charge readers of this CPS a fee. The Postal Service may charge a fee for issuing certificates, using Postal Service CA services, verifying certificates (e.g., per each online certificate status protocol transaction), and accessing Postal Service CA data.

Currently, the Postal Service CA does not technically support the online certificate status protocol (OCSP), however, support of this protocol is planned for the future.

2.6 Publication and Repository

2.6.1 **Publication of Certification Authority Information**

When the Postal Service public key infrastructure (PKI) enters phase 3 production, the Postal Service CA office will make available a repository that contains any, all, a subset, or a superset of the following for certificates issued by the Postal Service CA:

- a. Issued certificates that reference this CPS.
- b. A certificate revocation list.
- c. The certificate issued by the Postal Service root that contains the public key by which the authenticity of a published certificate can be verified.

- d. Past and current versions of the Postal Service CPS.
- e. Other relevant information relating to certificates referencing this CPS.

In addition, the Postal Service maintains an internal repository unavailable to the public. All issued certificates and other related information are securely stored in this protected internal repository.

2.6.2 Frequency of Publication

The Postal Service CA office will publish and maintain all information set forth in section 2.6.1 (Publication of Certification Authority Information) in a repository. This information will be published promptly after such information is available to the Postal Service CA. Certificates referencing this CPS are published promptly, both in the internal repository and public repository, upon the subscriber's acceptance of the certificate. The Postal Service CA office will publish information about revoked certificates in accordance with section 4.4.9 (Certificate Revocation List Issuance Frequency), unless otherwise negotiated with the Postal Service CA. On a case-by-case basis, the Postal Service will consider issuing certificates that will not be published in the Postal Service's public repository.

2.6.3 Access Controls

The following rules apply to the reading of the public repository:

- a. When the Postal Service PKI enters phase 3 production, the repository will be available substantially on a read-only basis, 24 hours per day, 7 days per week, subject to reasonable scheduled maintenance. *Substantially* means access is available for 95 percent of the time.
- b. Unless explicitly required by the subscriber, the Postal Service CA does not impose access controls on the reading of:
 - Certificates.
 - Certificate status information.
 - This CPS.
 - Past and current versions of the Postal Service CPS.

With regard to modifying either the internal or public repository, only trusted employees (see section 5.2.1, Trusted Roles) can access the internal repository if, and only if, required in performance of their official duties.

2.6.4 Repositories

When technically supported, online repositories will be available to the public through the lightweight directory access protocol (LDAP). The addresses of the repositories will be available from the Postal Service CA or approved RAs. Phase 1 production does not technically support LDAP access.

2.7 Compliance Audit

2.7.1 Frequency of Certification Authority Compliance Review

The Postal Service CA will undergo an annual audit to demonstrate compliance with this Postal Service CPS. An initial audit of the Postal Service CA will begin no later than 6 months after phase 3 production. In addition, the Postal Service CA should be audited any time that a significant change in the Postal Service CA equipment or Postal Service CPS or CA operations is made, whichever occurs first, to demonstrate continuing compliance with this CPS. If the results of an audit report recommend remedial actions, then the Postal Service will initiate corrective action within a reasonable time following receipt of such audit report.

2.7.2 Identity and Qualifications of Reviewer

The Postal Service Office of the Inspector General (OIG) is responsible for overseeing audits of all Postal Service computer systems. The auditor will be an accountant with demonstrated expertise in computer security or a computer security professional. The auditor must be knowledgeable with audit methodology, audit standards, PKI technologies, and security issues. The Postal Service OIG will oversee performance of the internal audit functions while an independent public accounting firm (licensed as a certified public accountant) will perform external audit functions. (See section 2.7.4, Scope of Audit, for internal and external audit functions.)

2.7.3 Auditor's Relationship to Audited Party

The auditors, both internal and external, will be independent of the Postal Service CA. The auditors will not have any conflict of interest with the audited party, as defined by the American Institute of Certified Public Accountants.

2.7.4 Scope of Audit

The external auditors will perform a compliance audit, which produces a report and an opinion on the service that the Postal Service CA provides to its subscribers and relying parties. Specifically, the compliance audit will test compliance of the Postal Service CA operations with the policies and procedures set forth in this Postal Service CPS. Management and external auditors will agree on a set of control objectives with which to assess the Postal Service CA.

The internal auditors, under the direction of the OIG, will assess the compliance of the CA's operations to:

- a. Postal Service corporate guidelines.
- b. Efficiency and effectiveness of the CA's operations.

- c. Effectiveness of management controls.
- d. Risks and threats associated with the CA.

The internal and external auditor's separate reports describe issues uncovered during the audit and will recommend actions to Postal Service management for correcting the issues.

2.7.5 **Actions Taken as a Result of Deficiency**

The auditors will note in the compliance audit, any discrepancies between the operations of the Postal Service CA and the stipulations of the Postal Service CPS and affiliated certificate policies. Upon receipt of a compliance audit that details any deficiencies, the Postal Service CA management group will use reasonable measures to correct the deficiencies in an expeditious manner in accordance with the risks posed by the discrepancy and the impact of its correction upon the certificate-using community.

Depending upon the severity of risk posed by the discrepancy, the Postal Service may:

- a. Continue to operate as usual.
- b. Continue to operate, but at a lower assurance level (pending correction of any problems).
- c. Suspend operation. Before CA operations are suspended, the Postal Service will revoke all certificates issued by the Postal Service CA and issue new certificates to subscribers when the deficiency is corrected.

The CA must inform the policy authority (see section 2.1.6, Policy Authority Obligations) of any actions taken in response to a compliance audit. The auditors and the policy authority will reassess the situation within an appropriate time interval. Upon reassessment, if the deficiencies are deemed to have been corrected, the Postal Service CA will continue or resume service accordingly.

2.7.6 **Communication of Results**

The auditors will report the results of all compliance audits to the Postal Service CA management at the address in section 1.4.2 (Contact Person). The Postal Service will make audit results available to relying parties, subscribers, business partners, and others upon written request and approval of the request. The Postal Service reserves the right to deny a request to release audit results to any requestor without penalty to the Postal Service.

2.8 Confidentiality

2.8.1 Types of Information to Be Kept Confidential

Subscriber Registration Data. For the purpose of proper administration of certificates, the Postal Service certification authority or an agent thereof may request non-certificate information (e.g., credit card number, home phone number, and social security number), to be used in the lifecycle management of certificates. In the event that this type of information is required, it will be handled as confidential and access will be restricted to those with an official need to access that information in performance of his or her official duties. This information may be made available with the prior written consent of the subscriber or if required by law. In addition, maintenance of any confidential information must be in compliance with the Privacy Act, and any Privacy Act notice promulgated in connection with specific records and specific applications.

Subscriber Private Keys. Under no circumstances will the Postal Service CA have access to the private keys, used for encryption purposes, of any subscriber to whom it issues certificates, after the certificate is issued without a specific agreement regarding the custody and safekeeping of the subscriber's private key. Under no circumstances will the Postal Service CA have access to or perform a storage function for the subscriber's private signing key.

Certification Authority and Registration Authority Private Keys. Private keys held by the Postal Service CA that are used to sign certificates and certificate revocation lists (CRL), as well as private keys held by authorized registration authorities to sign certificate requests are held in the strictest confidence.

2.8.2 Types of Information Not Considered Confidential

Information either appearing in the issued certificates, CRLs, OCSP responses, or capable of being gathered from public sources is not considered confidential. In addition, any information received from a third party who lawfully acquired it and who is under no obligation restricting its disclosure is not considered confidential. This CPS, certificates issued under this CPS, any associated revocation or certificate status information, and affiliated certificate policies are not considered confidential. A subscriber's distinguished name, which may include the subscriber's common name and electronic mail address, is not considered confidential.

2.8.3 Disclosure of Certificate Revocation and Suspension Information

The Postal Service CA is the authorized source for revocation and suspension information for certificates within its purview. The Postal Service makes this information available to subscribers and relying parties through a CRL. Revocation reason codes may be provided through the approved revocation mechanism (e.g., the reasonCode in an X.509 version 2 certificate

revocation list) and are not considered confidential. Aside from the information contained in the certificate revocation list entry extension, no other information concerning the revocation is routinely disclosed.

2.8.4 **Release to Law Enforcement Officials**

The Postal Service CA will not disclose confidential information, unless such disclosure is due to either of the following:

- a. The law, federal rule or regulation, or court order requires the release of the information.
- b. The subscriber authorized the release of the information.

2.8.5 **Release as Part of Civil Discovery**

The Postal Service CA will not disclose confidential certificate-related information unless the disclosure is due to either of the following:

- a. The law, federal rule or regulation, or court order requires the release of the information.
- b. The subscriber authorized the release of the information.

2.8.6 **Disclosure upon Owner's Request**

The Postal Service CA will release confidential certificate-related information with the prior written consent of the subscriber.

2.8.7 **Other Information Release Circumstances**

The Postal Service CA will not disclose confidential certificate-related information, unless the release is due to either of the following:

- a. The law, federal rule or regulation, or court order requires the release of the information.
- b. The subscriber authorized the release of the information.

2.9 **Intellectual Property Rights**

Certificate applicants (and, upon acceptance, subscribers) represent and warrant that all information, such as the applicant's distinguished name and usage domain, supplied in the certificate application process is accurate and does not infringe upon or violate in any way the trademarks, service marks, trade name, company names, or any other intellectual property right of any third party. Certificate applicants (and, upon acceptance, subscribers) will defend, indemnify, and absolve the Postal Service CA from all financial responsibility for any claims of loss or damage resulting from an infringement or violation. Any legal fees incurred by the Postal Service resulting from a claim will be paid by the offending certificate applicant (and, upon acceptance, certificate holder).

Certificates and certificate revocation lists issued by the Postal Service certification authority are the property of the Postal Service. This CPS is the property of the Postal Service. The distinguished names used to represent entities within the Postal Service CA domain in the directory and in certificates issued to subscribers within that domain may include a relative distinguished name for the Postal Service and, as such, are the property of Postal Service.

3 Identification and Authentication

3.1 Initial Registration

Subject to the requirements noted below, certificate applicants should submit their applications and credentials to a Postal Service-approved RA. The specific credentials required to authenticate an applicant may vary, depending on the type of certificate the applicant is requesting. Examples of the types of credentials that may be required are provided in sections 3.1.8 (Authentication of Sponsoring Organization Identity), 3.1.9 (Authentication of Individual Identity [No Affiliation]), and 3.1.10 (Authentication of Individual [Affiliated Certificate]).

3.1.1 Types of Names

The Postal Service CA requires the use of the following:

- a. An X.500 naming convention.
- b. An X.500 directory distinguished name format in the subject and issuer fields of the subscriber, registration authority, and certification authority X.509 certificates.

3.1.2 Name Meanings

[No stipulation.]

3.1.3 Rules for Interpreting Various Name Forms

[No stipulation.]

3.1.4 Name Uniqueness

New subscribers are issued a distinguished name that is unique from any other name issued by or on behalf of the Postal Service.

3.1.5 Name Claim Dispute Resolution Procedures

When there is a conflict in distinguished names, a modification to the submitted name may be used to make the name unique. In the final resolution of claim disputes, all affected parties waive all claims of loss arising from the Postal Service CA's decision to assign or to reassign a specific

subscriber name to a certificate applicant or to decline to issue a certificate. The Postal Service CA has the authority to make the final decision.

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

Each certificate applicant and, upon acceptance, each subscriber represents that:

- a. Their submission and use of a subject name and all other information connected or related to the certificate application does not infringe on the intellectual property rights or any other right of any third parties.
- b. They are not intending to, and will not, use the subject name for any unlawful purpose.

Each certificate applicant and subscriber will indemnify the Postal Service CA in respect of all claims, demands, actions, costs, expenses, loss and damage with regard to any breach of this warranty.

The Postal Service certification authority is not obligated to seek evidence of trademarks, court orders, or any other right to use the subject name prior to issuance. The Postal Service CA is not obligated to issue or to reissue a certificate with a particular subject name even if the certificate application contains a registered trademark owned by the certificate applicant or for which the applicant has submitted a trademark registration application.

3.1.7 **Verification of Possession of Private Key**

The user is required to prove possession of the private key that corresponds to the public key in the request by submitting a self-signed certificate request.

3.1.8 **Authentication of Sponsoring Organization Identity**

Valid authentication methods for an organization may include a subset, all, or a superset of the following:

- a. The organization's articles of incorporation.
- b. An authorization letter with company letterhead and seal, signed by a corporate officer.
- c. A third party's confirmation of business entity information.
- d. A review of the applicant's authorization records against third-party business databases or independent callbacks.

At its sole discretion, the Postal Service may amend its list of acceptable authentication methods.

3.1.9 **Authentication of Individual Identity (No Affiliation)**

The Postal Service issues certificates only to individuals who have submitted to a proofing process. A subscriber making a certificate request should present an easily recognized form of picture identification. The Postal Service will accept any of the following credentials as a valid form of identification:

- a. Driver's license.
- b. State-issued, non-driver identification.
- c. Military identification card.
- d. Passport (domestic or foreign).

The Postal Service also requires a second form of identification, which may include one of the following:

- a. Utility bill bearing the applicant's name and home address.
- b. Telephone bill bearing the applicant's name and home address.
- c. Tax statement bearing the applicant's name and home address.
- d. Mortgage statement bearing the applicant's name and home address.

At its sole discretion, the Postal Service may amend the lists of acceptable primary and secondary credentials.

3.1.10 **Authentication of Individual (Affiliated Certificate)**

In some instances, the Postal Service certification authority may delegate the identification and authentication of affiliated individuals to responsible individuals within the affiliated individual's organization. The Postal Service must first authenticate the responsible individual in accordance with section 3.1.9 (Authentication of Individual Identity [No Affiliation]), and the sponsoring organization in accordance with section 3.1.8 (Authentication of Sponsoring Organization Identity).

Once the responsible individual and the sponsoring organization are authenticated by the Postal Service, the responsible individual will authenticate affiliated individuals on behalf of the Postal Service CA. Responsible individuals will proof affiliated individuals in accordance with the proofing requirements stipulated in a certificate policy for which the responsible individual is authorized to perform the proofing function, and which is supported by the Postal Service CA.

3.1.10.1 **Duties of Responsible Individuals**

The Postal Service CA requires the responsible individual to issue and manage certificates for the sponsoring organization. This requires the responsible individual to properly authorize subscribers to receive certificates and notify the RA or the Postal Service CA of an affiliation change or termination.

3.2 Routine Rekey

When a certificate expires, the subscribers will reapply for a new certificate, following the same process and procedures for initial registration.

3.3 Rekey After Revocation

When a certificate is revoked, the subscriber will reapply for a new certificate, following the same process and procedures for initial registration.

3.4 Revocation Request

A revocation request may be submitted electronically via the Universal Registration system or by an approved registration authority. The identity of a person submitting a revocation request in any other manner (e.g. physically or via telephone) is authenticated by the Postal Service CA or the appropriate RA.

4 Operational Requirements

The Postal Service has established a process for requesting and receiving a certificate to ensure that certificates are issued only to properly authenticated individuals or entities. Once a certificate is delivered and accepted, Postal Service CA operations must manage the process of suspending, revoking, or renewing certificates as required. The Postal Service CA records and monitors security-related activities to ensure the integrity of the certificate process.

4.1 Certificate Application

A certificate applicant must complete a certificate application in a format prescribed by the Postal Service CA and, where applicable, enter into a subscriber agreement with the Postal Service CA. The RA accepts, reviews, and approves or rejects all applications. The act of completing the application process equals the subscriber's consent for the Postal Service to issue the certificate.

4.2 Certificate Issuance

Upon successful completion of the subscriber identification and authentication process in accordance with chapter 3 (Identification and Authentication) of this certification practice statement, and complete and final approval of the certificate application, the Postal Service CA will issue the requested certificate, notify the applicant, and make the certificate available to the applicant.

At the discretion of the Postal Service, the Postal Service CA may refuse to issue a certificate to any person, organization, or device, without incurring any liability or responsibility for any loss or expenses arising as a result of the refusal.

4.3 Certificate Acceptance

After the Postal Service certification authority has generated a certificate, the Postal Service CA requires the subscriber to accept or reject the certificate. If the subscriber does not take action on the certificate, the certificate will remain in a suspended status. However, at its sole discretion, the Postal Service may revoke any certificate that an applicant hasn't accepted within a specified time. The validity period for the certificate begins on the date of issue and not the date of acceptance.

4.4 Certificate Suspension and Revocation

4.4.1 Who Can Request Revocation

Only a trusted individual or the certificate holder (see chapter 10, Glossary) is permitted to request revocation of a certificate issued in accordance with this CPS.

4.4.2 Circumstances for Revocation

4.4.2.1 Permissive Revocation

A subscriber may request revocation of his or her certificate at any time for any reason. A sponsoring organization (where applicable) may request the revocation of the certificate of any affiliated individual or device at any time for any reason.

4.4.2.2 Required Revocation

A subscriber or responsible individual must promptly request revocation of a certificate, if any of the following occurs:

- a. Any of the information on the certificate changes or becomes obsolete.
- b. The private key or the media holding the private key associated with the certificate is, or is suspected of having been, compromised.
- c. An affiliated person is no longer affiliated with the sponsoring organization.

The Postal Service CA will revoke a certificate as follows:

- a. If the subscriber makes a request.
- b. If the subscriber fails to meet its material obligations under this CPS, any applicable certificate policy, or any other agreement, regulation, or law applicable to the certificate that may be in force.
- c. If the Postal Service obtains knowledge or reasonable suspicion that a subscriber's private key has been compromised.
- d. If the Postal Service CA determines that the certificate was not properly issued in accordance with this CPS or any applicable certificate policy.

- e. If the Postal Service determines that the subscriber has not accepted the certificate in a timely manner.

If the Postal Service CA ceases operations, all certificates issued by the Postal Service CA will be revoked before the date that the Postal Service CA ceased operations.

4.4.3 Procedure for Revocation Request

A subscriber requests revocation of the subscriber's certificate by submitting a revocation request electronically using the Universal Registration system. If the subscriber is unable to access the Universal Registration system, then the subscriber may contact an authorized RA in-person. After phase 3 production, a subscriber will also be able to call a customer help desk to request revocation of the subscriber's certificate.

4.4.3.1 Certificate Revocation List and Repository Update

After the CA has received a revocation request, the certificate revocation list and certificate status database in the internal repository is automatically updated, minimally, by close of business the following business day to reflect the revocation. The Postal Service CA audits and archives all revocation requests and the resulting actions.

4.4.4 Revocation Request Grace Period

Requests for revocation will only be accepted during business hours. The requests will be processed by the close of business on the next business day after receiving the request for revocation. Postal Service business hours for phase 1 are 11 a.m. to 7 p.m. Eastern Standard Time, Monday through Friday, except on Federal holidays or during outages due to system upgrades, routine maintenance, or other unexpected events.

4.4.5 Circumstances for Suspension

The Postal Service CA initially places a certificate in a suspended status until the subscriber accepts it. There are no distinct procedures for certificate suspension after the Postal Service CA releases a certificate into operation.

Note: A compromised certificate must be revoked rather than suspended.

4.4.6 Who Can Request Suspension

[Reserved for future use.]

4.4.7 Procedure for Suspension Request

[Reserved for future use.]

4.4.8 **Limits on Suspension Period**

The suspension period is limited to the time between when the Postal Service CA issues the certificate, to when the subscriber accepts the certificate. At the discretion of the Postal Service, the Postal Service may revoke a certificate that a subscriber has not accepted within a prescribed time after the certificate is issued.

4.4.9 **Certificate Revocation List Issuance Frequency**

The certificate revocation list will be updated daily, Monday through Friday, except on Federal holidays.

4.4.10 **Online Revocation and Status Checking Availability**

A certificate status checking database in the internal repository is available substantially (i.e., access is available 95 percent of the time) 7 days per week and 24 hours per day. The database is updated upon processing the certificate revocation request in accordance with section 4.4.4 (Revocation Request Grace Period).

4.4.11 **Certificate Revocation List Checking Requirements**

Relying parties should check the status of the certificate before using or relying on it. This may include checking the certificate revocation list or the online revocation status database via online certificate status protocol (OCSP) when technically supported.

4.4.12 **Online Revocation and Status Checking Availability**

When the Postal Service repository technically supports an online certificate status database, the Postal Service CA will update the database as soon as reasonably possible, but in no event later than the terms prescribed in section 4.4.4 (Revocation Request Grace Period). Phase 1 production does not technically support either the online certificate status protocol (OCSP) or LDAP retrieval of a CRL. At the discretion of the Postal Service CA management, the Postal Service CA will electronically mail CRLs to approved recipients.

4.4.13 **Online Revocation Checking Requirements**

Relying parties should check the status of the certificate before relying on it. This may include checking the CRL or checking the online revocation status database via OCSP when it is available. Phase 1 production does not technically support OCSP.

4.4.14 **Other Forms of Revocation Advertisements Available**

The Postal Service sponsors only the following two revocation advertisements:

- a. Certificate revocation list.
- b. Online revocation checking database, when it becomes available.

4.4.15 **Checking Requirements for Other Forms of Revocation Advertisements**

The Postal Service sponsors only the following two revocation advertisements:

- a. Certificate revocation list.
- b. Online revocation checking database, when it becomes available.

4.4.16 **Special Requirements Regarding Key Compromise**

See section 4.8.2 (Key Compromise Plan).

4.5 **Computer Security Audit Procedures**

The Postal Service CA equipment automatically records, for purposes of audit, events as described in section 4.5.1 (Types of Events Recorded), whether the event is attributable to human action or automatically invoked by the equipment. At a minimum, the following information is recorded:

- a. The type of event and the time the event occurred.
- b. For some event types, such as certificate application or certificate revocation requests, the transaction success or failure, the source or destination of a message, or the disposition of a created object (i.e., a filename).

When possible, the audit data is automatically collected. When this is not possible, personnel will record transactions in a logbook, beginning on or before phase 3 production.

Phase 1 production poses no audit requirements on the responsible individual or his or her RA equipment.

4.5.1 **Types of Events Recorded**

The Postal Service CA records the following events:

- a. Installation.
- b. Modification.
- c. Accesses.
- d. Requests.
- e. Responses.

- f. Actions (e.g., creation, signing, suspension, or revocation).
- g. Operations (e.g., backup, system errors, or recovery).
- h. Publications.

The auditing capabilities of the underlying equipment operating system are enabled during installation. The Postal Service CA equipment can audit routine system operations such as backup and restore, as well as capture events causing system errors.

The Postal Service CA application records the following:

Requests

- a. Certificate creation, modification, and revocation requests.
- b. Certificate receipt acknowledgments.
- c. Postal Service key compromise notices.

Actions performed in response to these requests and in support of the normal operation of the application

- a. Certificate and certificate revocation list creation.
- b. Accesses to the Postal Service CA databases.
- c. Any signing or encryption performed by the Postal Service CA.

Responses to requests and publication of data

- a. Certificates.
- b. Certificate revocation lists.

All, a subset, or a superset of the types of events listed in section 4.5.1 (Types of Events Recorded) are recorded in phase 1 production.

4.5.2 **Frequency of Audit Log Processing**

The Postal Service CA signs audit logs daily.

4.5.3 **Period for which Audit Logs are Kept**

The Postal Service keeps an archive of the audit trail files for 10 years and 6 months. At its discretion, the Postal Service may choose to keep all or a subset of audit logs for an extended period of time.

4.5.4 **Protection of Audit Logs**

The electronic audit log system includes mechanisms to protect the log files from unauthorized viewing, modification, or deletion. The audit log is digitally signed for storage, open for read access, and to the extent possible, is not open for modification by any human or computer process. The system administrator has the ability to delete the monthly consolidated audit log, after it's archived and at the discretion of the Postal Service.

4.5.5 **Audit Log Backup Procedures**

The Postal Service backs up the audit log at least once every business day. The Postal Service periodically ships a copy of the audit log backup off-site for storage in a geographically distinct area from the CA secure facility.

4.5.6 **Audit Collection System**

The audit log collection system is not external to the CA equipment. The audit agent is a separate module bundled within the CA application. Audit processes are invoked at system startup and cease only at system shutdown.

4.5.7 **Notification of Audit Subjects**

The Postal Service is not required to notify subscribers that an event is being audited. The Postal Service is not required to provide real time alerts to the event-causing subject for any audited event. The Postal Service, at its discretion, may choose to notify an event-causing subject of an audited event. This CPS does not address which events require notification.

4.5.8 **Vulnerability Assessments**

The certification authority, security authorities, and other operating personnel observe for attempts to violate the integrity of the certificate management system, including the equipment, physical location, and personnel. In phase 3 production, the Postal Service will check the daily audit log for anomalies as evidence of a violation, such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses. The Postal Service selects an independent third party to perform a vulnerability assessment.

At a minimum, the vulnerability assessment addresses the following:

- a. Operating system vulnerabilities.
- b. Physical system vulnerabilities.
- c. Adequacy of audit and logging procedures.
- d. Adherence to this certification practice statement and security policy.
- e. Disaster recovery preparedness.
- f. Personnel screening procedures.
- g. Network vulnerability (if connected to a network).

4.6 Records Archival

The Postal Service certification authority and registration authorities will keep confidential, the subscriber's personal and corporate information submitted on an application for a certificate. The Postal Service will not release information outside of the Postal Service without prior written consent from the subscriber, unless otherwise required by law. This policy does not apply to information appearing in certificates or to information available from public sources.

4.6.1 Types of Events Recorded

At the discretion of the Postal Service, the following data and files are archived by (or on behalf of) the Postal Service CA:

- a. All computer security audit data.
- b. All certificate application data.
- c. All certificates, CRLs, or certificate status records generated.
- d. Key histories (key information that may not be captured by the certificate revocation list such as CA key).

4.6.2 Retention Period for Archive

The Postal Service will make its CA certificate, other issued certificates, and certificate revocation lists available through an archive for a minimum of 10 years and 6 months, or as otherwise negotiated at the discretion of the Postal Service. Signatories or relying parties have the long-term responsibility for preserving the records needed to validate signatures indefinitely. Signatories or relying parties may retain or archive the certification paths needed to substantiate signatures, or have signed documents time-stamped or notarized as required.

4.6.3 Protection of Archive

The Postal Service protects archive media either by physical security alone, or a combination of physical security and cryptographic protection. Precautions are taken for environmental threats such as temperature, humidity, and magnetism. Only Postal Service authorized individuals can view the archived records.

4.6.4 Archive Backup Procedures

The Postal Service backs up the archives and stores them in a fireproof container, both on-site and off-site.

4.6.5 Requirements for Time-stamping of Records

The CA equipment automatically time-stamps records to be archived.

4.6.6 **Archive Collection System (Internal or External)**

The archive collection system is internal to the CA workstation.

4.6.7 **Procedures to Obtain and Verify Archive Information**

During the compliance audit required by this CPS, the auditor verifies the integrity of both copies of the archives. If the auditor finds that either copy is corrupt or damaged in any way, the archive is replaced with a duplicate of the undamaged archive.

4.7 **Key Changeover**

4.7.1 **Root Public Key**

The Postal Service certification authority root public key is valid for 20 years. At its discretion, the Postal Service may replace the root key before it expires in response to changes in technology that necessitate its replacement.

4.7.2 **Changeover Period**

There will be a key changeover period where the Postal Service CA phases out usage of the old private key. The Postal Service CA will stop signing certificates with its current private key, if the current private key is in the last 10 years of its active lifetime. Beginning at the start of the last 10 years, the CA will sign certificates with the newly generated private key. This allows the Postal Service CA time (key changeover period) to phase out certificates signed with the CA's old private key. The Postal Service CA follows this process for each of its root signing keys.

4.8 **Compromise and Disaster Recovery**

4.8.1 **Disaster Recovery Plan**

The Postal Service is developing a plan to help recover from a disaster and resume normal business operations. The disaster recovery plan will include a complete and periodic test of readiness. This plan will be complete before transitioning to phase 3 production.

4.8.2 **Key Compromise Plan**

Certification Authority or Registration Authority Private Key. Before transitioning to phase 3 production, the Postal Service CA will have in place a key compromise plan. The plan will be initiated when the Postal Service declares a compromise of either the private signing key used by the Postal Service CA to issue certificates or the private key of any authorized RA.

Once the Postal Service declares a compromise of either of these keys, the Postal Service will notify affected certificate holders.

Subscriber Private Key. When a subscriber becomes aware of any actual or suspected compromise in his or her private key, the subscriber is obligated to notify the Postal Service CA, his or her designated registration authority, or responsible individual immediately, and to request the revocation of his or her certificate. When a RA becomes aware of a compromised certificate within its purview, the RA must also request that the Postal Service CA revoke the compromised certificate.

After the Postal CA revokes a certificate, the subscriber may request a new certificate. The subscriber must reapply for certificates, using the same procedures as a new applicant.

4.9 Certification Authority Cessation of Services

In the event that the Postal Service CA ceases operation, all subscribers, sponsoring organizations, and authorized RAs will be promptly notified. In addition, all CAs with cross-certification agreements will be promptly notified that the Postal CA has ceased operation. All certificates issued by the Postal Service CA, referencing this CPS, will be revoked no later than the time of termination.

5 Physical, Procedural, and Personnel Security Controls

This chapter describes the non-technical security controls of a physical, procedural, and personnel nature for the Postal Service CA and related activities. These controls are intended to provide a secure environment for key generation, certificate applicant authentication, certificate issuance, certificate suspension or revocation, audit, and archival activities. The controls must function as intended to prevent the creation of certificates with incorrect information or the compromise of the Postal Service CA private key.

5.1 Physical Security Controls

The Postal Service has implemented appropriate physical security controls to restrict access to CA hardware and software (including the server, workstations, and any external cryptographic hardware modules or tokens) used in connection with providing CA services. The Postal Service limits access to hardware and software, to those personnel performing in a trusted role as described in section 5.2.1 (Trusted Roles). The Postal Service controls access through the use of electronic access controls, mechanical combination lock sets, or deadbolts. The access controls are manually or electronically monitored for unauthorized intrusion at all times.

5.2 Procedural Controls

5.2.1 Trusted Roles

A *trusted role* refers to one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously.

All employees, contractors, and consultants of the Postal Service CA (collectively, *personnel*) that have access to or control over cryptographic operations that may materially affect the Postal Service CA's issuance, use, suspension, or revocation of certificates, including access to restricted operations of the Postal Service CA's repository, serve in a trusted role. Such personnel include, but are not limited to, system administration personnel, database administration personnel, data handling and support staff, and security staff who are designated to oversee the Postal Service CA's operations.

5.2.2 **Number of Persons Required Per Task**

To ensure that one person acting alone cannot circumvent safeguards, responsibilities at the Postal Service CA server are shared among multiple roles and individuals. Each account on the Postal Service CA server has capabilities commensurate with the role of the account holder.

5.2.3 **Identification and Authentication for Each Role**

Identification and authentication mechanisms, such as passwords and tokens, are used to control account access for each role. All access by each role to accounts requires password or token identification and authentication.

5.3 **Personnel Controls**

5.3.1 **Background and Qualifications**

The Postal Service CA and RAs enforce approved personnel and management policies. These policies provide reasonable assurance of the trustworthiness, competence, and satisfactory performance of employees in a manner consistent with this CPS.

5.3.2 **Background Investigation**

The Postal Inspection Service oversees an appropriate investigation of all personnel who serve in trusted roles before they are employed and periodically thereafter as necessary. This is to verify personnel trustworthiness and competence in accordance with the requirements of this CPS, the Postal Service CA's personnel practices, or equivalent practices or requirements.

5.3.3 **Training Requirements**

All trusted personnel attend focused training before performing their duties. In addition to technical training, trusted personnel receive training with regard to data handling to ensure confidential information is handled in compliance with the Privacy Act and any Privacy Act notice promulgated in connection with specific records and specific applications.

After the initial training, new personnel may be trained by existing operators of the equipment.

5.3.4 **Retraining Frequency and Requirements**

All administrators will receive new training when a major system upgrade is implemented.

5.3.5 Sanctions for Unauthorized Actions

If unauthorized actions are committed by an administrator, that administrator will be barred from serving in a trusted role. The Postal Service will take additional disciplinary actions as deemed necessary.

5.3.6 Contracting Personnel Requirements

All contracting personnel should follow guidelines comparable to section 5.3.1 (Background and Qualifications).

5.3.7 Documentation Supplied to Personnel

Before transitioning to phase 3 production, personnel involved in Postal Service CA operations will receive necessary documentation from Postal Service CA management to define their duties and responsibilities.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Trusted personnel generate CA keys in hardware tokens from which the private keys of the Postal Service CA cannot be extracted. End users generate their own private and public keys in either hardware or software. The Postal Service recommends that subscribers use the native capabilities of Netscape Navigator with a version 4.04, 4.05, 4.06, 4.61, or 4.71 browser or Microsoft Internet Explorer with a version 5.00.2614.3500, 5.00.2929.0000, or 5.00.2919.6307 browser to generate the key pair. Other browser versions should work with the Postal Service PKI. *Subscribers who choose other browser versions do so at their own risk.* Subscribers are wholly responsible for maintaining the security health of their browsers. The Postal Service is not liable for any losses that result from the exploitation of a subscriber's browser or workstation. For approved applications, the RA workstation may generate the end-users' keys on their behalf.

6.1.2 Private Key Delivery to Entity

The subscriber generates the private key and stores it on the subscriber's workstation or token. Alternatively, an authorized RA delivers the private key to the subscriber via encrypted floppy or smart card.

6.1.3 Subscriber Public Key Delivery to Certification Authority

The subscriber delivers the public key to the Postal Service CA via diskette or via a secure electronic transaction process.

6.1.4 Certification Authority Public Key Delivery to Users

Subscribers automatically receive the Postal Service root CA certificate and organization cross-certificate during the certificate download process. In phase 3 production, users will be able to get a copy of the Postal Service's root CA certificate and organization cross-certificate either by downloading them from a Postal Service Web site or by retrieving them via LDAP.

6.1.5 **Key Sizes**

The Postal Service CA keys are equal to 1024-bit Rivest-Shamir-Adleman (RSA) algorithm public keys or greater.

6.1.6 **Key Usage Purposes**

The Postal Service CA provides dual key support. End entities may use their respective key pairs for digital signature, non-repudiation, or encryption purposes. The Postal Service CA uses its keys for signing certificates and certificate revocation lists.

6.2 **Private Key Protection**

The subscriber is responsible for protecting his or her private key from unauthorized disclosure via, minimally, password protection.

6.2.1 **Standards for Cryptographic Module**

The certification authority's RSA and digital signature algorithm (DSA) private keys are stored in a cryptographic module that meets the requirements of a FIPS 140-1 level 3 device. The Elliptic Curve Digital Signature Algorithm (ECDSA) signing key is stored in software.

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

The Postal Service root private key's activation data is split among multiple trusted personnel.

6.2.3 **Private Key Escrow**

The Postal Service signature private key is not escrowed.

6.2.4 **Private Key Backup**

The CA's backup private key is stored encrypted on physical media.

6.2.5 **Private Key Archival**

The CA's private signature key is not archived.

6.2.6 **Private Key Entry into Cryptographic Module**

The CA's private key is generated in a cryptographic module.

6.2.7 **Method of Activating Private Key**

Activating the Postal Service root private key requires the participation of multiple trusted personnel who each control a portion of the activation data.

6.2.8 **Method of Deactivating Private Key**

The Postal Service root private key is deactivated by logging out of the private key module or removing the private key's hardware device.

6.2.9 **Method of Destroying Private Key**

The Postal Service will securely destroy the private key. When any private key is destroyed, the Postal Service revokes the corresponding certificate in accordance with section 4.4.2 (Circumstances for Revocation).

6.3 **Other Aspects of Key Pair Management**

6.3.1 **Public Key Certificate Archival**

The public keys of the Postal Service CA root are archived for a minimum of 10 years and 6 months after the certificate expires or is revoked. The public keys of other certificate holders are archived as expressed in agreements between the Postal Service and the designated application owner.

6.3.2 **Usage Periods for the Public and Private Keys (Key Replacement)**

The active lifetime for the root Postal Service CA's public key is 20 years. The Postal Service CA will stop signing certificates with its current private key when the current private key is in the last 10 years of its active lifetime. At its discretion, the Postal Service may choose to replace its root public and private key pairs earlier in response to technology changes.

6.4 **Activation Data**

Activation data refer to data values other than keys that are required to operate cryptographic modules and that need to be protected, such as a personal identification number. Both the subscriber's and the CA's private keys should be stored in encrypted form and must be unlocked when the subscriber or CA enters activation data.

6.4.1 **Activation Data Generation and Installation**

The CA's activation data is randomly generated and distributed.

6.4.2 **Activation Data Protection**

Passwords are encrypted when they are not in use. In addition, subscribers and CA trusted personnel must keep activation data private. If a subscriber circumvents or deactivates the password mechanism or discloses the activation data, the subscriber is fully liable for any losses that arise from the unauthorized use of his or her private key.

6.4.3 **Other Aspects of Activation Data**

The Postal Service CA and authorized RAs select strong passwords in accordance with Postal Service policies and regulations for password selection.

6.5 **Computer Security Controls**

The Postal Service CA servers protect all CA system information from unauthorized access either through protections provided by the operating system, or through a combination of operating system, PKI application, physical safeguards, and network safeguards.

6.6 **Lifecycle Technical Controls**

The CA system was developed in conformance with Postal Service Handbook AS-805, *Information Systems Security*.

6.7 **Network Security Controls**

The networks on which the Postal Service CA and its internal repository reside are protected from unauthorized users through a series of firewalls. Further protection is provided via the use of hardened operating systems. *Hardening* an operating system is a method employed to allow only necessary services to be active on the system.

6.8 **Cryptographic Module Engineering Controls**

The Postal Service CA cryptographic module is a FIPS 140-1 level 3 certified module.

7 Certificate and Certificate Revocation List Policies

To ensure global compatibility and conformity to public key standards, the Postal Service CA uses the ITU-T X.509 version 3 digital certificate. As a minimum, an X.509 certificate contains:

- a. The subject's information.
- b. The issuer's signature algorithm identifier.
- c. The issuer's signature over the certificate.

The Postal Service CA also uses the ITU-T X.509 version 2 certificate revocation lists. An X.509 version 2 certificate revocation list contains a signed list of certificates that the Postal Service CA has revoked and the reasons for revocation along with the date and other information. The profiles for both certificates and certificate revocation lists conform to RFC 2459, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile*.

Note: At the discretion of the Postal Service, private extensions may be supported as required by specific applications.

8 Certificate Policy Administration

8.1 Certificate Policy Change Procedures

8.1.1 **Changes Not Requiring Notice**

The Postal Service is not required to notify subscribers or change the version number of this CPS, if the changes, in the judgment of the Postal Service CA, have no or minimal impact on the users of certificates and certificate revocation lists issued by the Postal Service CA. For example, typographical corrections and changes to contact information require no notice.

8.1.2 **Changes Requiring Notice**

The Postal Service is required to notify subscribers or change the version number of this CPS, if the changes, in the judgment the Postal Service CA, may have a significant impact on users of certificates and certificate revocation lists issued by the Postal Service CA. The most recent copy of the Postal Service CPS will supersede all previous versions and impose a legal obligation on subscribers, the Postal Service CA, and all affected registration authorities.

8.2 Publication and Notification Procedures

Before making changes to this CPS, the Postal Service will notify subscribers of upcoming changes on the Postal Service Internet (www.usps.com/cps). When the CPS is updated, a subscriber will be able to revoke his or her certificate within 15 days without obligating the certificate holder to the terms of the updated CPS. A subscriber's decision not to request a revocation of his or her certificate within the 15 days following publication of an updated CPS constitutes acceptance of the updated CPS.

8.3 Certificate Policy Approval Procedures

The Postal Service CA management must approve any subsequent changes to this CPS.

9 Acronyms and Abbreviations

The following acronyms and abbreviations are used in this document.

CA	certification authority
CP	certificate policy
CPS	certification practice statement
CRL	certificate revocation list
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standards
IETF	Internet Engineering Task Force.
NIST	National Institute of Standards and Technology
OCSP	online certificate status protocol
OID	object identifier
PA	policy authority
PIN	Personal Identification Number
PKI	public key infrastructure
RA	Registration Authority
RSA	Rivest-Shamir-Adleman Algorithm
RSP	repository service provider
WWW	World Wide Web

10 Glossary

This glossary explains standard terms used in this handbook.

Activation Data. Private data, other than keys, required to access cryptographic modules or storage areas.

Affiliated Individual. An affiliated individual is the subject of a certificate that is affiliated with a sponsor approved by the certification authority (such as an employee affiliated with an employer). Certificates issued to affiliated individuals are intended to be associated with the sponsor and the responsibility for authentication lies with the sponsor.

Authenticate. Relates to a situation where one party has presented an identity and claims to be that identity. Authentication enables another party to gain confidence that the claim is legitimate.

Certificate. A data record that, at a minimum: (a) identifies the CA issuing it; (b) names or otherwise identifies its subscriber; (c) contains a public key that corresponds to a private key under the control of the subscriber; (d) identifies its operational period; and (e) contains a serial number and is digitally signed by the CA issuing it.

Certificate Holder. See subscriber.

Certificate Policy (CP). An explicit set of rules governing the application of a certificate to a specific application or community.

Certificate Rekey. The process whereby a subscriber with an existing key pair and certificate receives a new certificate for a new public key, following the generation of a new key pair.

Certificate Revocation List (CRL). A time-stamped list of revoked certificates that have been digitally signed by a certification authority.

Certification Authority (CA). A certification authority, also known as a certificate authority, is an entity that is responsible for authorizing and causing the issuance of a certificate.

Certification Authority Key Changeover. The procedure used by a certification authority (CA) to replace its active private and public key pairs.

Certification Practice Statement (CPS). A statement of the practices that a certification authority employs in issuing, suspending, revoking, and renewing certificates and providing access to same, in accordance with specific requirements (i.e., requirements specified in this CPS or requirements specified in a contract for services).

Compromise. The unauthorized disclosure of information or a violation of a system's security policy.

Delegated Proofing. The authorization of a non-Postal Service employee to perform identity verification processes in accordance with guidelines either furnished by or approved by the Postal Service.

Digital Signature. A digital signature is a string of bits associated with a collection of data (e.g., a file, document, message, or transaction); this string of bits can only be generated by the holder of a private key, but can be verified by anyone with access to the corresponding public key. Note that some algorithms include additional steps (e.g., one-way hashes or time stamps) in this basic process.

Distinguished Name. A set of attribute value assertions concerning the distinguished values of a particular entity that identify an entity (e.g., countryName=US, organizationName=PostalService, role=OrgRA, or commonName=JohnDoe).

End Entity. See subscriber.

Federal Information Processing Standards (FIPS). These are Federal standards that prescribe specific performance requirements, practices, formats, communications protocols, etc. for hardware, software, data, telecommunications operation, etc. Federal agencies are expected to apply these standards as specified unless a waiver has been granted in accordance to agency waiver procedures.

Internet Engineering Task Force (IETF). A large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

Key Pair. Two mathematically related keys, having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (2) even knowing one key, it is computationally infeasible to discover the other key.

Level of Assurance. The level of assurance or *assurance level* represents categories of practices followed by the CA or an authorized RA in validating the identity of the certificate applicant and binding this identity to the corresponding public key. The assurance level may affect the degree of confidence placed in the resultant certificate.

Mutual Authentication. Parties at both ends of a communication activity authenticate each other (see authenticate).

Object Identifier (OID). A unique numeric or alphanumeric identifier that unambiguously names an object and is registered with an internationally-recognized standards organization.

Online Certificate Status Protocol (OCSP). A protocol that enables applications to determine the revocation state of an identified certificate. OCSP was designed to provide more timely revocation information than is possible with the periodic issuance of a certificate revocation list.

Operational Period of a Certificate. The certificate's period of validity. It typically begins on the date the certificate is issued (or such later date as specified in the certificate), and ends on the date and time it expires as noted in the certificate, unless it is revoked or suspended earlier.

Organization Cross-Certificate. A certificate that identifies a subordinate CA within the Postal Service's PKI hierarchy, is signed by the Postal Service's trusted root CA, and is used to create a trusted path to the trusted root CA.

Out-of-band. Communication between parties using a means or method that differs from the current method of communication (e.g., one party using U.S. Postal Service mail to communicate with another party where current communication is online communication).

Personal Identification Number (PIN; password; passphrase). An access control mechanism, usually a character string, that is kept confidential by its user and is required to gain entrance to a system resource.

PKIX. An IETF working group developing technical specifications for PKI components based on X.509 version 3 certificates.

Policy Authority (PA). The entity responsible for creation and promulgation of the CPS.

Postal Service. Abbreviated form of the United States Postal Service.

Private Extension. An X.509-compliant extension that is defined and used by a PKI community to convey information unique to that community.

Private Key. Either the key of a signature key pair used to create a digital signature, or the key of an encryption key pair used to decrypt encrypted data. In both instances, this key must be kept secret.

Proofing. The process of validating a set of identity criteria for a certificate applicant in order to gain assurance that the identity of the subject named in the digital certificate fairly represents the identity of the certificate applicant.

Public Key. Either a key of a signature key pair used to verify a digital signature, or the key of an encryption key used to encrypt data. The public key is usually provided via a certificate issued by a CA and is often obtained by accessing a repository.

Public Key Infrastructure. All mechanisms, including personnel, facilities, policies, procedures, operational practices, and technical infrastructure, required to securely issue, manage, and distribute certificate-based public keys.

Registration Authority (RA). An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a registration authority is delegated certain tasks on behalf of a certification authority).

Relying Party. A recipient of a digitally-signed message who is authorized to rely on a certificate to verify the digital signature on a message.

Repository. A database containing information and data relating to certificates and a CA.

Repository Service Provider (RSP). An entity that maintains a repository accessible to the public [or at least to relying parties] for the purpose of obtaining copies of certificates and certificate validation information.

Responsible Individual. A person designated by a sponsor to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.

Revoke a Certificate. To prematurely end the operational period of a certificate from a specified time forward.

Root Public Key. A self-signed certificate that occupies the top of the trust chain within a hierarchical PKI.

Sponsor. An organization with which a subscriber is affiliated (e.g., as an employee, user of a service, or business partner customer).

Subject. An entity, such as an individual or network device, which either has a public key certified in a certificate or who triggers an audit event (audit subject). Also referred to as a *subscriber*.

Subscriber. A person or entity who (1) is the subject named or identified in a certificate issued to such person or entity and (2) holds a private key that corresponds to a public key listed in that certificate, and (3) the person or entity to whom digitally-signed messages verified by reference to such certificate are to be attributed (see subject).

Subscriber Agreement. A contract that represents the complete agreement and understanding between the certification authority and the subscriber.

Suspend a Certificate. To temporarily suspend the operational period of a certificate for a specified time or from a specified time forward.

Trusted Individual. One who performs in a trusted role.

Trusted Role. One whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously

Trustworthy System. Computer hardware, software, and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions, and (4) adhere to generally accepted security procedures.

Valid Certificate. A certificate that (1) a CA has issued, (2) the subscriber listed in it has accepted, (3) has not expired, and (4) has not been revoked.