Citizen and Commerce Class Common Certificate Policy
Version 2.1

March 11, 2008

1 Introduction

1.1 Overview

This Certificate Policy (CP) defines requirements for certificates accepted by the U.S. Federal Government for the purpose of authenticating citizens and commercial enterprises for many electronic services. Recognition of Entity CAs under this policy is based on policy mapping and review by the FPKI Policy Authority's Certificate Policy Working Group. Appendix B specifies requirements of this policy that only apply to the Citizen and Commerce Class Common Certification Authority (C4CA).

Any use of or reference to this CP outside the purview of the Federal PKI Policy Authority is completely at the using party's risk.

This CP is consistent with [RFC 3647], the Internet Engineering Task Force Public Key Infrastructure X.509 (IETF PKIX) Certificate Policy and Certification Practices Framework.

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

1.2 Document name and identification

This policy is identified by the following OID:

citizen-and-commerce-approved ::= 2.16.840.1.101.3.2.1.14.2

The U.S. Federal PKI will issue cross-certificates that assert this policy OID to certificate providers whose policies satisfy these requirements. The citizen-and-commerce-approved OID indicates that the Federal PKI Policy Authority, or its agent, has reviewed the provider's policy and determined that it meets the requirements for this policy.

1.3 PKI participants

1.3.1 PKI authorities

The following roles are relevant to the administration and operation of the Citizen and Commerce Class Common (C4) Certification Authority.

1.3.1.1 Federal Chief Information Officers Council

The Federal CIO Council comprises the Chief Information Officers of all cabinet level departments and other independent agencies. The Federal CIO Council has established the framework for the interoperable FPKI and oversees the operation of the organizations responsible for governing and promoting its use. In particular, this CP was established under the authority of and with the approval of the Federal CIO Council.

1.3.1.2 Federal PKI Policy Authority (FPKIPA)

The Federal PKI Policy Authority (FPKIPA) is a group of U.S. Federal Government Agencies (including cabinet-level Departments) chartered by the Federal CIO Council. The FPKIPA owns this policy and represents the interest of the Federal CIOs. The FPKIPA is responsible for:

- The Citizen and Commerce Class Common Certificate Policy,
- The Federal PKI Architecture X.509 Certification Practice Statement – Part 4: X.509 Certification Practice Statement for the Citizen and Commerce Class Common (C4) Certification Authority,
- Accepting applications from Entities desiring to interoperate using the C4CA,
- After an Entity is authorized to interoperate using the C4CA, ensuring continued conformance of that Entity with applicable requirements as a condition for allowing continued interoperability using the C4CA.

The FPKIPA will execute a Memorandum of Agreement (MOA) with each cross-certified Entity setting forth the respective responsibilities and obligations of both parties and the mappings between the certificate levels of assurance contained in this CP and those in the Entity CP. (When the Entity belongs to a sovereign nation, the United States Department of State may execute the MOA or delegate the authority to execute the MOA on its behalf.)

1.3.1.3 FPKI Operational Authority (FPKI OA)

The FPKI Operational Authority is the organization that operates and maintains the C4CA on behalf of the U.S. Government, subject to the direction of the FPKIPA.

1.3.1.4 FPKI Operational Authority Program Manager

The Program Manager is the individual within the FPKI Operational Authority who has principal responsibility for overseeing the proper operation of the C4CA including the C4CA repository, and selecting the FPKI Operational Authority Staff. The Program Manager is selected by the FPKI Operational Authority and reports to the FPKIPA. The FPKI Operational Authority Program Manager must hold a Top Secret security clearance.

1.3.1.5 Entity Principal Certification Authority (CA)

The Principal CA is a CA within a PKI that has been designated to cross-certify directly with the C4CA (e.g., through the exchange of cross-certificates). The Principal CA issues either end entity certificates, or CA certificates to other Entity or external party CAs, or both. Where the Entity operates a hierarchical PKI, the Principal CA is typically the Entity Root CA. Where the Entity operates a mesh PKI, the Principal CA may be any CA designated by the Entity for cross-certification with the C4CA.

It should be noted that an Entity may request that the C4CA cross-certify with more than one CA within the Entity; that is, an Entity may have more than one Principal CA. Additionally, this CP may refer to CAs that are "subordinate" to the Principal CA. The use of the term "subordinate CA" shall encompass any CA under the control of the Entity that has a certificate issued to it by the Entity Principal CA or any CA subordinate to the Principal CA, whether or not the Entity employs a hierarchical or other PKI architecture.

1.3.1.6 Citizen and Commerce Class Common Certification Authority (C4CA)

The C4CA is the entity operated by the FPKI Operational Authority that is authorized by the Federal PKI Policy Authority to create, sign, and issue public key certificates to Principal CAs. As operated by the FPKI Operational Authority, the C4CA is responsible for all aspects of the issuance and management of a certificate including:

- Control over the registration process,
- The identification and authentication process,
- The certificate manufacturing process,
- Publication of certificates,
- Revocation of certificates,
- Re-key of C4CA signing material, and
- Ensuring that all aspects of the C4CA services and C4CA operations and infrastructure related to certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP.

1.3.1.7 Certificate status servers

PKIs may optionally include an authority that provides status information about certificates on behalf of a CA through on-line transactions. In particular, PKIs may include OCSP responders to provide on-line status information. Such an authority is termed a Certificate Status Server (CSS). Where the CSS is identified in certificates as an authoritative source for revocation information, the operations of that authority are considered within the scope of this CP. Examples include OCSP servers that are identified in the authority information access (AIA) extension. OCSP servers that are locally trusted, as described in [RFC 2560], are not covered by this policy.

1.3.2 Registration authorities

The RA collects and verifies each subscriber's identity and information for inclusion in the subscriber's public key certificate. The FPKI Operational Authority acts as the RA for the C4CA, and performs its function in accordance with a CPS approved by the Federal PKI Policy Authority. Entity CAs designate their own RAs. The requirements for RAs in the C4CA and Entity PKIs are set forth elsewhere in this document.

1.3.3 Subscribers

A subscriber is the user or device to whom or to which a certificate is issued. C4CA subscribers include only FPKI Operational Authority personnel and, when determined by the Federal PKI Policy Authority, network or hardware devices. Note that CAs are sometimes technically considered "subscribers" in a PKI. However, the term "subscriber" as used in this document does not refer to CAs.

1.3.4 Relying parties

A relying party uses a subscriber's certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the subscriber. The relying party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. A relying party may use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use.

This CP makes no assumptions or limitations regarding the identity of relying parties. While relying parties are generally subscribers, relying parties are not required to have an established relationship with the C4CA or an Entity CA.

1.3.5 Other participants

The C4CA and Entity CAs may require the services of other security, community, and application authorities. If required, the C4CA or Entity CPS shall identify the parties, define the services, and designate the mechanisms used to support these services.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Relying parties determine whether or not certificates that satisfy this policy are appropriate for their application, and whether certificate status information needs be verified before use.

1.4.2 Prohibited certificate uses

No stipulation.

1.5 Policy administration

1.5.1 Organization administering the document

The Federal PKI Policy Authority is responsible for all aspects of this CP.

1.5.2 Contact person

Questions regarding this CP shall be directed to the Chair of the Federal PKI Policy Authority, whose address can be found at http://www.cio.gov/fpkipa.

1.5.3 Person determining CPS suitability for the policy

The Certification Practices Statement must conform to the corresponding Certificate Policy. The Federal PKI Policy Authority is responsible for asserting whether the C4CA CPS conforms to this CP. Entities must designate the person or organization that asserts that their CPS(s) conforms to their CP(s).

In the case of the C4CA the determination of suitability shall be based on an independent compliance auditor's results and recommendations. See section B.8 for further details.

1.5.4 CPS approval procedures

The FPKI Operational Authority shall submit the C4CA CPS and the results of a compliance audit to the FPKIPA for approval. The FPKIPA shall vote to accept or reject the CPS. If rejected, the FPKI Operational Authority shall resolve the identified discrepancies and resubmit to the FPKIPA. The C4CA is required to meet all facets of the policy. The FPKIPA will not issue waivers.

Entity CAs shall submit their CPS and the results of their compliance audit to the appropriate authority (see section 1.5.3) for approval. An Entity CA's CPS shall be required to meet all facets of its policy. Waivers, while discouraged, may be permitted in order to meet urgent unforeseen operational requirements. Any waivers issued by Entity CAs are considered changes to the corresponding CP, and may result in revocation of the cross-certificate by the FPKIPA.

2 Publication and repository responsibilities

2.1 Repositories

The FPKI Operational Authority shall operate repositories to support C4CA operations.

Entity PKIs are responsible for operation of repositories to support their PKI operations

2.2 Publication of certification information

This CP shall be made publicly available on the FPKIPA website (see http://www.cio.gov/fpkipa). The CPS for the C4CA will not be published; a redacted version of the C4CA CPS will be publicly available from the FPKIPA website (see http://www.cio.gov/fpkipa).

2.3 Time or frequency of publication

This CP and any subsequent changes shall be made publicly available within thirty days of approval.

2.4 Access controls on repositories

The FPKI Operational Authority shall protect any repository information not intended for public dissemination or modification. Certificates and certificate status information in the C4CA repository shall be publicly available through the Internet.

Access to information in Entity CA repositories shall be determined by the Entity pursuant to the rules and statutes that apply to that Entity. Certificates and certificate status information in the Entity repository should be publicly available through the Internet wherever reasonable. At a minimum, the Entity repositories shall make CA certificates and CRLs issued by the Entity PKI and CA certificates issued to the Entity PKI available to Federal relying parties.

3 Identification and authentication

The CA is responsible for authenticating the identity of the subject before certificate issuance.

3.1 Naming

The CA is responsible for ensuring the uniqueness of certificate subject names for all certificates issued by that CA. Under no circumstances shall additional certificates containing the same subject name be issued to a different subscriber (person, role, or organization).

3.2 Initial identity validation

The identity may be established in any of the following manners:

1. The identity may be established through in-person appearance at the credential provider, or its agent, with physical credentials (e.g., driver's license or birth certificate).
2. The identity may be established using procedures similar to those used when applying for consumer credit and authenticated through information in consumer credit databases or government records, such as:
    - the ability to place calls from or receive phone calls at a given number; or
    - the ability to obtain mail sent to a known physical address.
3. Where an ongoing business relationship with the credential provider or a partner company (e.g., a financial institution, airline, or retail company) exists, the identity may be authenticated through information derived from the business relationship such as:
    - the ability to obtain mail at the billing address used in the business relationship; or
    - verification of information established in previous transactions (e.g., previous order number); or
    - the ability to place calls from or receive phone calls at a phone number used in previous business transactions.

3.3 Identification and authentication for re-key requests

For cross-certificates issued by the C4CA, after an Entity CA certificate has been revoked other than during a renewal or update action, the Entity CA is required to go through the initial cross-certification process to obtain a new certificate.

There is no stipulation for certificates issued by Entity CAs.

3.4 Identification and authentication for revocation request

When a request to revoke a certificate is received, the CA is responsible for authenticating the identity of the requester.

4 Certificate life-cycle operational requirements

4.1 Certificate application

CAs that wish to cross certify with the Federal Government under this policy shall follow the process described on http://www.cio.gov/fpkipa. Entities applying for C4CA cross-certification are responsible for providing accurate information on their certificate applications.

This policy makes no stipulation regarding certificate application procedures for subscribers.

4.2 Certificate application processing

Entity CPs may specify procedures to verify information in certificate applications.

4.3 Certificate issuance

No stipulation.

4.4 Certificate acceptance

No stipulation.

4.5 Key pair and certificate usage

No stipulation.

4.6 Certificate renewal

No stipulation.

4.7 Certificate re-key

No stipulation.

4.8 Certificate modification

No stipulation.

4.9 Certificate revocation and suspension

This policy requires CAs to maintain and distribute certificate status information until certificate expiration. When a certificate's status changes, the new status must be available to relying parties within 72 hours.

Certificate status information must be distributed using at least one of the following mechanisms: X.509 CRLs; or the Online Certificate Status Protocol (OCSP). If a certificate is not covered by an X.509 CRL, the certificate must explicitly specify the authoritative OCSP server using the Authority Information Access extension.

4.10 Certificate status services

No stipulation.

4.11 End of subscription

No stipulation.

4.12 Key escrow and recovery

CA private keys are never escrowed. There is no stipulation for subscriber's private keys.

5 Facility, management, and operational controls

The CA shall take adequate measures to ensure the security of its operations.

5.1 Physical controls

No stipulation.

5.2 Procedural controls

No stipulation.

5.3 Personnel controls

No stipulation.

5.4 Audit logging procedures

No stipulation.

5.5 Records archival

Entity CAs shall maintain a record of the facts of registration (including revocation) for a minimum of seven years and six months beyond the expiration or revocation (whichever is later) of the certificate. Entities shall also comply with their respective records retention policies in accordance with whatever laws apply to those Entities.

5.6 Key changeover

No stipulation.

5.7 Compromise and disaster recovery

If operations are disrupted by disaster or other unexpected events, notice should be provided to the Federal PKI Policy Authority shortly thereafter. Otherwise, there is no stipulation for Entity CAs beyond the requirements of the applicable MOA.

5.8 CA or RA termination

The CA shall inform the Federal PKI Policy Authority prior to planned termination or suspension of CA operations.

6 Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

CAs and CSSes shall generate private keys used to sign certificates and certificate status information in cryptographic modules validated against FIPS 140 Level 2 (or higher). This policy makes no stipulation regarding the generation of subscriber private keys.

6.1.2 Private key delivery to subscriber

No stipulation.

6.1.3 Public key delivery to certificate issuer

No stipulation.

6.1.4 CA public key delivery to relying parties

No stipulation.

6.1.5 Key sizes

CAs and CSSes that generate certificates, CRLs, and other status information (e.g., OCSP responses) under this policy shall use signature keys of at least 1024 bits for RSA or DSA, and at least 160 bits for ECDSA. Certificates, CRLs, and other status information that expire after 12/31/2011 shall be generated with at least a 2048 bit RSA or DSA key, or at least 224 bits for ECDSA.

CAs and CSSes that generate certificates, CRLs, and other status information under this policy shall use the SHA-1, SHA-224, SHA-256, SHA-384, or SHA-512 hash algorithm when generating digital signatures. Signatures on certificates, CRLs, and other status information issued after 12/31/2011 shall be generated using, at a minimum, SHA-224.

End entity certificates that expire before 12/31/2013 shall contain public keys that are at least 1024 bits for RSA, DSA, or Diffie-Hellman, or 160 bits for elliptic curve algorithms. End entity certificates that expire on or after 12/31/2013 shall contain public keys that are at least 2048 bits for RSA, DSA, or Diffie-Hellman, or 224 bits for elliptic curve algorithms.

6.1.6 Public key parameters generation and quality checking

No stipulation.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

CA certificates issued under this policy are required to include the key usage extension. Certificates containing CA public keys that are used to verify certificates shall assert *keyCertSign*; certificates containing CA public keys that are used to verify CRLs shall assert *cRLSign*.

There is no stipulation for end entity certificates.

6.2 Private key Protection and cryptographic module engineering controls

CA and CSS private keys used to sign certificates and certificate status information shall be maintained in cryptographic modules validated against FIPS 140 Level 2 (or higher).

This policy makes no stipulation regarding the protection of subscriber private keys.

6.3 Other aspects of key pair management

No stipulation.

6.4 Activation data

No stipulation.

6.5 Computer security controls

No stipulation.

6.6 Life cycle technical controls

No stipulation.

6.7 Network security controls

No stipulation.

6.8 Time-stamping

No stipulation.

7 Certificate, CRL, and OCSP profiles

This policy requires issuance of X.509 version 3 certificates.

8 Compliance audit and other assessments

No stipulation.

9 Other business and legal matters

9.1 Fees

The Federal PKI Policy Authority reserves the right to charge a fee to each Entity in order to support operations of the C4CA.

9.2 Financial responsibility

This CP contains no limits on the use of any certificates issued by the C4CA or by Entity CAs. Rather, entities acting as relying parties shall determine what financial limits, if any, they wish to impose for certificates used to complete a transaction.

9.3 Confidentiality of business information

C4CA information not requiring protection shall be made publicly available. Federal PKI Policy Authority access to Entity information will be addressed in the MOA with that Entity. Public access to Entity information shall be determined by the respective Entity.

9.4 Privacy of personal information

Confidentiality requirements (if any) are determined by agreement between subscriber and CA.

9.5 Intellectual property rights

The FPKI Operational Authority will not knowingly violate intellectual property rights held by others.

9.6 Representations and warranties

9.6.1 CA representations and warranties

This policy requires CAs to issue certificates, maintain and distribute certificate status information, and protect the private key(s) used to sign certificates and certificate status information.

9.6.2 RA representations and warranties

No stipulation.

9.6.3 Subscriber representations and warranties

This policy requires subscribers to inform the CA if they believe their private key(s) have been compromised, stolen, or lost.

9.6.4 Relying party representations and warranties

No stipulation.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

Federal agencies agreeing to use these certificates do not have a fiduciary relationship with CAs operating under this policy. The existence of a fiduciary relationship (if any) between CAs and subscribers is determined by contract or agreement between those parties.

9.8 Limitations of liability

The U.S. Government shall not be liable to any party, except as determined pursuant to the Federal Tort Claims Act (FTCA), 28 U.S.C. 2671-2680, or as determined through a valid express written contract between the Government and another party.

For Entity CAs, no stipulation.

9.9 Indemnities

Under no circumstances will a Federal agency agree to indemnify a CA issuing certificates under this policy. CAs and subscribers may reach their own agreements as to indemnification.

9.10 Term and termination

9.10.1 Term

This CP becomes effective when approved by the FPKI Policy Authority. This CP has no specified term.

9.10.2 Termination

Termination of this CP is at the discretion of the FPKI Policy Authority.

9.10.3 Effect of termination and survival

No stipulation.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

9.12.1 Procedure for amendment

No stipulation.

9.12.2 Notification mechanism and period

This CP and any subsequent changes shall be made publicly available.

9.12.3 Circumstances under which OID must be changed

OIDs will be changed at the sole discretion of the FPKI Policy Authority.

9.13 Dispute resolution provisions

Any dispute arising with respect to this policy or certificates issued under this policy shall be resolved by the parties.

9.14 Governing law

The construction, validity, performance, and effect of certificates issued under this CP for all purposes shall be governed by United States Federal law (statute, case law, or regulation).

9.15 Compliance with applicable law

No stipulation.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force majeure

No stipulation.

9.17 Other provisions

No stipulation.

References

[FIPS 140-2] Security Requirements for Cryptographic Modules, May 25, 2001.

[RFC 2560] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, June 1999.

[RFC 3647] S. Chokhani, W. Ford, R. Sabett, C. Merrill, and S. Wu. Internet X.509 public key infrastructure certificate policy and certification practices framework, November 2003.

A Acronyms

AIA	Authority Information Access (certificate extension)
C4CA	Citizen and Commerce Class Common (C4) Certification Authority
CA	Certification Authority
CIO	Chief Information Officer
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSS	Certificate Status Server

DSA	Digital Signature Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS PUB	(US) Federal Information Processing Standards Publication
FPKI	Federal Public Key Infrastructure
FPKI OA	Federal Public Key Infrastructure Operational Authority
FPKIPA	Federal PKI Policy Authority
FTCA	Federal Tort Claims Act
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
MOA	Memorandum of Agreement
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	Policy Authority
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SHA	Secure Hash Algorithm

B Requirements for the C4CA

This appendix specifies requirements that only apply to the C4CA. The C4CA must satisfy all requirements specified in this appendix in addition to any requirements specified earlier in this document.

B.1 Introduction

See section 1.

B.2 Publication and repository responsibilities

See section 2.

B.3 Identification and authentication

B.3.1 Naming

B.3.1.1 Types of names

Certificates issued by the C4CA shall include a non-null subject DN.

B.3.1.2 Need for names to be meaningful

Names used in the certificates issued by the C4CA must identify the Entity CA, person, or object to which assigned.

B.3.1.3 Anonymity or pseudonymity of subscribers

The C4CA shall not issue anonymous certificates. CA certificates issued by the C4CA shall not contain anonymous or pseudonymous identities. The C4CA may issue pseudonymous certificates to support internal operations.

B.3.1.4 Rules for interpreting various name forms

No stipulation.

B.3.1.5 Uniqueness of names

See section 3.1.

B.3.1.6 Recognition, authentication, and role of trademarks

The FPKIPA shall resolve any name collisions or disputes regarding C4CA-issued certificates brought to its attention. Consistent with Federal policy, the C4CA will not knowingly use trademarks in names unless the subject has the rights to use that name.

B.3.2 Initial identity validation

B.3.2.1 Method to prove possession of private key

In all cases where the party named in a certificate generates its own keys that party shall be required to prove possession of the private key that corresponds to the public key in the certificate request.

B.3.2.2 Authentication of organization identity

Requests for C4CA certificates in the name of an organization shall include the organization name, address, and documentation of the existence of the organization. The FPKI Operational Authority shall verify the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the organization.

B.3.2.3 Authentication of individual identity

See section 3.2.

B.3.2.4 Non-verified subscriber information

No stipulation.

B.3.2.5 Validation of authority

For cross-certification, the FPKI Operational Authority shall validate the Entity CA representative's authorization to act in the name of the organization.

B.3.2.6 Criteria for interoperation

The FPKIPA shall determine the criteria for cross-certification with the C4CA.

B.3.3 Identification and authentication for re-key requests

B.3.3.1 Identification and authentication for routine re-key

In the event that an Entity Principal CA re-key is required, the C4CA will issue a new certificate to the Principal CA. Before issuance, the Entity Principal CA shall identify itself through use of its current signature key or the initial registration process. If it has been more than three years since an Entity Principal CA was identified as required in section B.3.2, identity shall be re-established through the initial registration process.

B.3.3.2 Identification and authentication for re-key after revocation

After an Entity CA cross-certificate has been revoked other than during a renewal or update action, the Entity CA is required to go through the initial cross-certification process to obtain a new certificate.

B.3.4 Identification and authentication for revocation request

When a request to revoke a certificate is received, the FPKI Operational Authority is responsible for authenticating the identity of the requester.

B.4 Certificate life-cycle operational requirements

B.4.1 Certificate application

The C4CA may issue end-entity certificates to trusted personnel where necessary for the internal operations of the C4CA. The C4CA will not issue end-entity certificates for any other reasons.

B.4.1.1 Who can submit a certificate application

For the C4CA, the certificate application shall be submitted to the FPKIPA by an authorized representative of the Entity CA.

B.4.1.2 Enrollment process and responsibilities

Entities applying for C4CA cross-certification are responsible for providing accurate information on their certificate applications. Upon issuance, each certificate issued by the C4CA shall be manually checked to ensure each field and extension is properly populated with the correct information before the certificate is delivered to the Entity.

B.4.2 Certificate application processing

For the C4CA, the FPKI OA must verify information in certificate applications as accurate before certificates are issued.

B.4.3 Certificate issuance

B.4.3.1 CA actions during certificate issuance

CA certificates created by the C4CA shall be checked to ensure that all fields and extensions are properly populated. After generation and verification, the FPKI Operational Authority shall post CA certificates in the C4CA directory system.

B.4.3.2 Notification to subscriber by the CA of issuance of certificate

No stipulation.

B.4.4 Certificate acceptance

B.4.4.1 Conduct constituting certificate acceptance

No stipulation.

B.4.4.2 Publication of the certificate by the CA

All CA certificates issued by the C4CA shall be published in the FPKIA repository.

B.4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

B.4.5 Key pair and certificate usage

No stipulation.

B.4.6 Certificate renewal

A certificate issued by the C4CA may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the subscriber name and attributes are unchanged.

B.4.7 Certificate re-key

No stipulation.

B.4.8 Certificate modification

No stipulation.

B.4.9 Certificate revocation and suspension

See section 4.9.

B.4.9.1 Circumstances for revocation

For the C4CA, a certificate shall be revoked when the binding between the Entity CA and the CA's public key defined within a certificate is no longer valid. There are three circumstances under which certificates issued by the C4CA shall be revoked:

- The first circumstance is when the Federal PKI Policy Authority requests revocation of a C4CA-issued certificate. This will be the normal mechanism for revocation in cases where the Federal PKI Policy Authority determines that an Entity PKI does not meet the Federal PKI policy requirements or certification of the Entity PKI is no longer in the best interests of the Federal Government.
- The second circumstance is when the Operational Authority receives an authenticated request from a previously designated official of the Entity responsible for the Principal CA.
- The third circumstance is when the C4CA Operational personnel determine that an emergency has occurred that may impact the integrity of the certificates issued by the C4CA. Under such circumstances, the following individuals may authorize immediate certificate revocation:
  - Chair, Federal PKI Policy Authority
  - Other personnel as designated by the Chair, Federal PKI Policy Authority.

The Federal PKI Policy Authority shall meet as soon as practicable to review the emergency revocation.

B.4.9.2 Who can request revocation

A C4CA certificate may be revoked upon direction of the Federal PKI Policy Authority or upon an authenticated request by a designated official of the Entity responsible for the Principal CA (such official or officials shall be identified in the MOA as authorized to make such a request).

B.4.9.3 Procedure for revocation request

Upon receipt of a revocation request involving a C4CA-issued certificate, the FPKI Operational Authority shall authenticate the request and apprise the Federal PKI Policy Authority. The Federal PKI Policy Authority may, at its discretion, take whatever measures it deems appropriate to verify the need for revocation. If the revocation request appears to be valid, the Federal PKI Policy Authority shall direct the FPKI Operational Authority to revoke the certificate.

B.4.9.4 Revocation request grace period

No stipulation.

B.4.9.5 Time within which CA must process the revocation request

No stipulation.

B.4.9.6 Revocation checking requirement for relying parties

No stipulation.

B.4.9.7 CRL issuance frequency (if applicable)

No stipulation except as specified in section 4.9.

B.4.9.8 Maximum latency for CRLs (if applicable)

No stipulation except as specified in section 4.9.

B.4.9.9 On-line revocation/status checking availability

No stipulation except as specified in section 4.9.

B.4.9.10 On-line revocation checking requirements

No stipulation.

B.4.9.11 Other forms of revocation advertisements available

No stipulation.

B.4.9.12 Special requirements related to key compromise

No stipulation.

B.4.9.13 Circumstances for suspension

Suspension shall not be used by the C4CA.

B.4.9.14 Who can request suspension

No stipulation.

B.4.9.15 Procedure for suspension request

No stipulation.

B.4.9.16 Limits on suspension period

No stipulation.

B.4.10 Certificate status services

No stipulation.

B.4.11 End of subscription

No stipulation.

B.4.12 Key escrow and recovery

Under no circumstances shall a C4CA signature key used to sign certificates or CRLs be escrowed. The C4CA shall not perform any encryption key recovery functions involving Entity CAs, and shall not store any information encrypted by the C4CA public key that may require key recovery capabilities. However, if encryption key pairs need to be issued by the C4CA covering repository system access or for other purposes, the FPKIPA shall publish applicable requirements for that purpose.

B.5 Facility, management, and operational controls

B.5.1 Physical controls

All C4CA equipment including cryptographic modules shall be protected from unauthorized access at all times.

B.5.1.1 Site location and construction

The location and construction of the facility housing the C4CA equipment shall be consistent with facilities used to house high value information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, shall provide protection against unauthorized access to the C4CA equipment and records.

B.5.1.2 Physical access

The C4CA equipment shall always be protected from unauthorized access. The security mechanisms shall be commensurate with the level of threat in the equipment environment.

Removable cryptographic modules, activation information used to access or enable cryptographic modules, and other sensitive CA equipment shall be placed in secure containers when not in use. A security check of the facility housing the C4CA equipment shall occur if the facility is to be left unattended. A person or group of persons shall be made explicitly responsible for making such checks.

B.5.1.3 Power and air conditioning

The C4CA shall have backup capability sufficient to automatically lock out input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. In addition, the C4CA directories (containing C4CA issued certificates and CRLs) shall be provided with uninterrupted power sufficient for a minimum of six hours operation in the absence of commercial power.

B.5.1.4 Water exposures

C4CA equipment shall be installed such that it is not in danger of exposure to water. Water exposure from fire prevention and protection measures (e.g., sprinkler systems) are excluded from this requirement.

B.5.1.5 Fire prevention and protection

No stipulation.

B.5.1.6 Media storage

C4CA media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic). Sensitive media shall be stored so as to protect it from unauthorized physical access.

B.5.1.7 Waste disposal

C4CA sensitive media and documentation that are no longer needed for operations shall be destroyed in a secure manner. For example, sensitive paper documentation shall be shredded, burned, or otherwise rendered unrecoverable.

B.5.1.8 Off-site backup

For the C4CA, full system backups sufficient to recover from system failure shall be made on a periodic schedule. Backups are to be performed and stored off-site not less than once per week. At least one full backup copy shall be stored at an off-site location separate from the C4CA equipment. Only the latest full backup need be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational CA.

B.5.2 Procedural controls

No stipulation.

B.5.3 Personnel controls

B.5.3.1 Qualifications, experience, and clearance requirements

The FPKIPA and the FPKI OA are the responsible and accountable authorities for the operation of the C4CA. All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity. For the C4CA, all trusted roles are required to be held by U.S. citizens. FPKI Operational Authority personnel acting in trusted roles shall hold TOP SECRET security clearances.

B.5.3.2 Background check procedures

No stipulation.

B.5.3.3 Training requirements

All personnel performing duties with respect to the operation of the C4CA shall receive comprehensive training in all operational duties, security principles and mechanisms, and system and CA software that they are expected to perform, use, or maintain, including disaster recovery and business continuity procedures.

Documentation shall be maintained identifying all personnel who received training and the level of training completed. Where competence was demonstrated in lieu of training, supporting documentation shall be maintained.

B.5.3.4 Retraining frequency and requirements

Individuals responsible for PKI roles shall be aware of changes (e.g., software or hardware upgrade, changes in automated security systems, and relocation of equipment) in the C4CA operation. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented.

Documentation shall be maintained identifying all personnel who received training and the level of training completed.

B.5.3.5 Job rotation frequency and sequence

For the C4CA, any job rotation frequency and sequencing procedures shall provide for continuity and integrity of the C4CA services.

B.5.3.6 Sanctions for unauthorized actions

The FPKI Operational Authority shall take appropriate actions where personnel have performed actions involving the C4CA or its repository not authorized in this CP, the C4CA CPS, or other procedures published by the FPKI Operational Authority.

B.5.3.7 Independent contractor requirements

Contractor personnel employed to perform functions pertaining to the C4CA shall meet the personnel requirements set forth in section B.5.3.1.

B.5.3.8 Documentation supplied to personnel

For the C4CA, documentation sufficient to define duties and procedures for each trusted role shall be provided to the personnel filling that role.

B.5.4 Audit logging procedures

Audit log files shall be generated for all events relating to the security of the C4CA. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with retention period for archive, section B.5.5.2.

B.5.4.1 Types of events recorded

A message from any source received by the C4CA requesting an action related to the operational state of the CA is an auditable event. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- The type of event,
- The date and time the event occurred,

- A success or failure indicator, where appropriate,
- The identity of the entity and/or operator that caused the event.

B.5.4.2 Frequency of processing log

Audit logs shall be reviewed as needed for cause. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the log. Actions taken as a result of these reviews shall be documented.

B.5.4.3 Retention period for audit log

No stipulation.

B.5.4.4 Protection of audit log

C4CA system configuration and procedures must be implemented together to ensure that:

- Only personnel assigned to trusted roles have read access to the logs;
- Only authorized people may archive audit logs; and,
- Audit logs are not modified.

The entity performing audit log archive need not have modify access, but procedures must be implemented to protect archived data from destruction prior to the end of the audit log retention period (note that deletion requires modification access).

The off-site storage location for audit logs shall be a safe, secure location separate from the CA equipment.

B.5.4.5 Audit log backup procedures

No stipulation.

B.5.4.6 Audit collection system (internal vs. external)

The audit log collection system may or may not be external to the C4CA system. Automated audit processes shall be invoked at system or application startup, and cease only at system or application shutdown. Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the FPKI Operational Authority Administrator shall determine whether to suspend C4CA operation until the problem is remedied.

B.5.4.7 Notification to event-causing subject

No stipulation.

B.5.4.8 Vulnerability assessments

C4CA personnel shall routinely assess whether the CA system or its components have been attacked or breached.

B.5.5 Records archival

B.5.5.1 Types of records archived

C4CA archive records shall be sufficiently detailed to establish the proper operation of the C4CA, or the validity of any certificate (including those revoked or expired) issued by the C4CA. At a minimum, archival data should include all relevant policy and procedural documentation, system configuration with modifications, certificate requests and issuance records, re-keying activities, and all audit records.

B.5.5.2 Retention period for archive

The C4CA must follow either the General Records Schedule established by the National Archives and Records Administration or an agency-specific schedule as applicable.

B.5.5.3 Protection of archive

No unauthorized user shall be permitted to write to or delete the archive. The contents of the archive shall not be released except in accordance with sections 9.3 and 9.4. Any subscribers involved in the transaction or their legally recognized agents may request release of individual transactions records.

Archive media shall be stored in a safe, secure storage facility separate from the C4CA itself. For the C4CA, archived records may be moved to another medium when authorized by the FPKI Operational Authority Administrator. If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site. Applications required to process the archive data shall also be maintained for a period determined by the Federal PKI Policy Authority for the C4CA.

Prior to the end of the archive retention period, the FPKI Operational Authority shall provide archived data and the applications necessary to read the archives to a Federal PKI Policy Authority approved archival facility, which shall retain the applications necessary to read this archived data.

B.5.5.4 Archive backup procedures

No stipulation.

B.5.5.5 Requirements for time-stamping of records

CA archive records shall be automatically time-stamped as they are created. The CPS shall describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.

B.5.5.6 Archive collection system (internal or external)

No stipulation.

B.5.5.7 Procedures to obtain and verify archive information

The contents of the archive shall not be released except as determined by the Federal PKI Policy Authority for the C4CA or as required by law. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents.

B.5.6 Key changeover

For the C4CA, key changeover procedures will establish key rollover certificates where a certificate containing the old public key will be signed by the new private key, and a certificate containing the new public key will be signed by the old private key.

B.5.7 Compromise and disaster recovery

If operations are disrupted by disaster or other unexpected events, notice should be provided to the Federal PKI Policy Authority shortly thereafter.

The FPKI OA shall notify the members of the FPKIPA if any of the following cases occur:

- Suspected or detected compromise of the C4CA systems
- Physical or electronic attempts to penetrate C4CA systems
- Denial of service attacks on C4CA systems
- Any incident preventing the C4CA from issuing CRL (or OCSP) notices within 24 hours of the time specified in the next update field of its currently valid CRL or OCSP revocation notice.

The FPKI OA shall reestablish operational capabilities as quickly as possible in accordance with procedures set forth in the C4CA CPS.

B.5.8 CA or RA termination

The CA shall inform the Federal PKI Policy Authority prior to planned termination or suspension of operations.

B.6 Technical security controls

B.6.1 Key pair generation and installation

In addition to the requirements specified in section 6.1, the C4CA shall sign certificates and CRLs using an RSA key that is at least 2048 bits or an elliptic curve key that is at least 224 bits and shall sign certificates and CRLs issued after 12/31/2010 using, at a minimum, SHA-224.

B.6.2 Private key protection and cryptographic module engineering controls

B.6.2.1 Cryptographic module standards and controls

See section 6.2.

B.6.2.2 Private key (n out of m) multi-person control

For the C4CA, two or more persons are required for the following tasks:

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

B.6.2.3 Private key escrow

See section B.4.12.

B.6.2.4 Private key backup

C4CA private signature keys shall be backed up under multi-person control, as specified in section B.6.2.2. At least one copy of the C4CA private signature key shall be stored off site. All copies of the CA private signature key shall be accounted for and protected in the same manner as the original.

B.6.2.5 Private key archival

C4CA-issued private signature keys shall not be archived. For private encryption (a.k.a. key management or key transport) keys, no stipulation.

B.6.2.6 Private key transfer into or from a cryptographic module

No stipulation.

B.6.2.7 Private key storage on cryptographic module

No stipulation.

B.6.2.8 Method of activating private key

For the C4CA, CA signing key activation requires multiparty control.

B.6.2.9 Method of deactivating private key

No stipulation.

B.6.2.10 Method of destroying private key

No stipulation.

B.6.2.11 Cryptographic module rating

No stipulation.

B.6.3 Other aspects of key pair management

No stipulation.

B.6.4 Activation data

No stipulation.

B.6.5 Computer security controls

For the C4CA, computer security technical requirements shall be commensurate with the outcome of a FIPS 199 assessment.

B.6.6 Life cycle technical controls

See section B.6.5 above.

B.6.7 Network security controls

See section B.6.5 above.

B.6.8 Time-stamping

Asserted times shall be accurate to within three minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events.

B.7 Certificate, CRL, and OCSP profiles

This policy requires issuance of X.509 version 3 certificates.

B.8 Compliance audit and other assessments

B.8.1 Frequency or circumstances of assessment

The C4CA shall be subject to a periodic compliance audit at least once per year.

B.8.2 Identity/qualifications of assessor

For the C4CA, the auditor must demonstrate competence in the field of compliance audits. At the time of the audit, the C4CA compliance auditor must be thoroughly familiar with the requirements that the Federal PKI Policy Authority imposes on the issuance and management of C4CA certificates. The compliance auditor must perform such compliance audits as a regular ongoing business activity.

B.8.3 Assessor's relationship to assessed entity

The compliance auditor must be organizationally independent from the owner of the CA.

B.8.4 Topics covered by assessment

The compliance audit of the C4CA shall verify that the FPKI Operational Authority is implementing all provisions of a CPS approved by the FPKI Policy Authority consistent with this CP. The audit shall also verify that the FPKI Operational Authority is implementing the relevant provisions of the MOAs between the FPKI Policy Authority and each Entity PKI.

B.8.5 Actions taken as a result of deficiency

When the compliance auditor finds a discrepancy between the way the C4CA is being operated and the requirements of this CP, the discrepancy shall be documented and provided to the FPKI OA for remediation.

B.8.6 Communication of results

No stipulation.

B.9 Other business and legal matters

See section 9.