



**C4CA Certificate Policy Change Proposal Number: 2010-01**

**To:** Federal PKI Policy Authority  
**From:** Certificate Policy Working Group  
**Subject:** Proposed modifications to the Citizen and Commerce Class Common Certification Authority (C4CA) Certificate Policy  
**Date:** August 5, 2010  
**Title:** Changes to bring the C4CA CP into alignment with recent operational changes to the FBCA CP.

**Version and Date of Certificate Policy Requested to be changed:**

Citizen and Commerce Class Common Certificate Policy, Version 2.1, March 11, 2008.

**Change Advocate's Contact Information:**

Name: Cheryl Jenkins  
Organization: GSA – FPKI MA  
Telephone number: 202-577-1441  
E-mail address: Cheryl.Jenkins@gsa.gov

**Organization requesting change:** Federal PKI Management Authority

**Change summary:** Bring the C4CA into operational alignment with the FBCA. Specifically:

- Clarify the purpose of archiving, and the archiving requirements for auditable events. Also, clarify that NARA and/or other applicable regulations apply.
- Permit remote administration of the C4CA and associated repositories by the appropriate Trusted Roles, so that C4CA Certificate Policy (CP) operational and security requirements are maintained.
- Permit the compliance audit against the full CPS to be conducted over three years as long as some of the key controls are examined annually.

**Background:** In 2008, the FPKIPA adopted a change to the FBCA CP to clarify the purpose of archives records and to list the specific data required to be archived.

In December, 2009, the FPKIPA adopted a change to the FBCA CP that allows Certification Authorities (CAs) to implement remote administration without degrading FBCA CP operational and security requirements.

In January, 2010, the FPKIPA adopted a change to the FBCA CP to further align federal policy to emerging industry trends and lessons learned about reasonable compliance audit that ensure trust and assurances are being maintained.

The FPKI MA would like to maximize the operational efficiency of the FPKI by aligning the different CAs they manage by adopting the three operational changes to the FBCA CP in the C4CA CP.

**Specific Changes:** The specific changes for each of the three C4CA CP changes are listed below in separate sections.

Text with ~~strikethrough~~ will be removed. Underlined text will be added.

### **There are two specific changes for clarification of archiving:**

1.) Remove last sentence of the first paragraph in section **B.5.4, *Audit Logging Procedures***, which requires all audit records to be archived.

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.~~

2.) Modify the list in Section **B.5.5.1, *Types of Events Archived***, to add audit events that should be archived and clarify audit reporting requirements.

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~~ compliance audit reports.

### **There are five specific changes in support of remote administration.**

#### **2.4 Access controls on repositories**

The FPKI Management 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. To promote consistent access to certificates and CRLs, the repository shall implement access controls and communication mechanisms to prevent modification or deletion of information.

#### **B.5.1 Physical controls**

All C4CA equipment including cryptographic modules and remote workstations used to administer the CA 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, as well as sites housing remote workstations used to administer the CA, 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, high security locks, 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, or remote workstations used to administer the CA, 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.5.4.4 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 location where the data was generated.

**There is one specific change for triennial audit.**

#### **B.8.1 Frequency or circumstances of assessment**

The C4CA shall be subject to a periodic compliance audit at least once per year. As an alternative to a full annual compliance audit against the entire CPS, the compliance audit of CAs and RAs may be carried out in accordance with the requirements as specified in the Triennial Audit Guidance document located at <http://www.idmanagement.gov/fpkipa/>.

#### **Estimated Cost:**

There is no financial cost associated with implementing this change.

#### **Risk/Impact:**

None. Positive impact is that operational requirements for the C4CA in the area of archive, audit and remote administration will be brought into alignment with the operational requirements of the Federal Bridge CA, making management of the FPKI CAs more efficient.

**Implementation Date:**

This change will be implemented immediately upon approval by the FPKIPA and incorporation into the C4CA Certificate Policy.

**Prerequisites for Adoption:**

There are no prerequisites.

**Plan to Meet Prerequisites:**

There are no prerequisites.

**Approval and Coordination Dates:**

Date presented to CPWG: August 5, 2010  
Date presented to FPKIPA: August 10, 2010  
Date of approval by FPKIPA: August 10, 2010