FBCA Policy Change Proposal Number: 2008-02

To: Federal PKI Policy Authority
From: FPKI Certificate Policy Working Group
Subject: Proposed modifications to the FBCA CP
Date: 24 June 2008

Title: Changes to FBCA CP to clarify the archive definition and how its records are intended to be used.

Version and Date of Certificate Policy Requested to be changed:
X.509 Certificate Policy for The Federal Bridge Certification Authority (FBCA) version 2.8, dated 15 February 2008.

Change Advocates Contact Information:
Cheryl Jenkins, GSA
(202) 577-1441
Cheryl.jenkins@gsa.gov

Organization requesting change: FPKI Management Authority

Background: Entities are developing archive management plans that include storage and retrieval options. The FBCA CP is not clear on archive management; hence, this ambiguity may prevent cost savings for each entity, per their interpretation of the policy. Specifically, it is not clear whether entities are to use archive records to literally restore PKI components, or use them to prove the PKI was operating properly (i.e., in accordance with its policies and practices). It is further unclear whether the FBCA CP allows entities to choose between restoring PKI components and verifying the validity of any certificate, as a means of demonstrating proper PKI operation. In addition, the FBCA CP seems to suggest that every auditable event should also be archived. This is onerous and results in massive storage requirements; therefore it is recommended that specific auditable events that should also be archived be added to the Archive table in 5.5.1. The CPWG examined each auditable event and identified those that should be archived. As a result, an alternate table that lists required data to be archived is included with this change proposal.

Change summary: Clarify the purpose or archiving and the archiving requirements for auditable events. Also, clarify that NARA and/or other applicable regulations apply.

Specific Changes: There are four specific changes listed below. Text with ~~strikethrough~~ will be removed. Underlined text will be added.

1.) Remove last sentence of the first paragraph in section 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 FBCA or Entity CAs. 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 5.5.2.~~

2.) Add text indicating that the requirements of NARA and/or other regulatory bodies must be followed. This text will be added to the beginning of section 5.5, *Records Archive*.

Executive branch agencies must follow either the General Records Schedules established by the National Archives and Records Administration or an agency-specific schedule as applicable. All other entities shall comply with their respective records retention policies in accordance with whatever laws apply to those entities.

3.) Clarify paragraph one of section 5.5.1, *Types of Events Archived*, regarding the purpose of archive and move the paragraph so that it becomes the second paragraph in the beginning of section 5.5, *Records Archive*.

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

FBCA or Entity CA archive records shall be sufficiently detailed as to verify that the FBCA or Entity CA was properly operated as well as verify the validity of any certificate (including those revoked or expired) issued by the FBCA or Entity CA

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

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

Data To Be Archived	**Rudimentary**	**Basic**	**Medium (all policies)**	**High**
CA accreditation (if applicable)	X	X	X	X
Certificate Policy	X	X	X	X
Certification Practice Statement	X	X	X	X
Contractual obligations	X	X	X	X

Data To Be Archived	**Rudimentary**	**Basic**	**Medium (all policies)**	**High**
Other agreements concerning operations of the CA	X	X	X	X
System and equipment configuration	X	X	X	X
Modifications and updates to system or configuration	X	X	X	X
Certificate requests	X	X	X	X
Revocation requests		X	X	X
Subscriber identity Authentication data as per Section 3.2.3		X	X	X
Documentation of receipt and acceptance of certificates (if applicable)		X	X	X
Subscriber Agreements		X	X	X
Documentation of receipt of tokens		X	X	X
All certificates issued or published	X	X	X	X
Record of CA Re-key	X	X	X	X
All CRLs issued and/or published		X	X	X
~~All Audit Logs~~	~~X~~	~~X~~	~~X~~	~~X~~
Other data or applications to verify archive contents		X	X	X
~~Documentation required by compliance auditors~~ Compliance Auditor reports		X	X	X
Any changes to the Audit parameters, e.g., audit frequency, type of event audited		X	X	X
Any attempt to delete or modify the Audit logs		X	X	X
Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)	X	X	X	X
All access to certificate subject private keys retained within the CA for key recovery purposes	X	X	X	X
All changes to the trusted public keys, including additions and deletions	X	X	X	X
The export of private and secret keys (keys used for a single session or message are excluded)	X	X	X	X
The approval or rejection of a certificate status change request		X	X	X
Appointment of an individual to a Trusted Role	X	X	X	X

Data To Be Archived	Rudimentary	Basic	Medium (all policies)	High
Destruction of cryptographic modules		X	X	X
All certificate compromise notifications		X	X	X
Remedial action taken as a result of violations of physical security		X	X	X
Violations of Certificate Policy	X	X	X	X
Violations of Certification Practice Statement	X	X	X	X

Estimated Cost:
There is no financial cost associated with implementing this change.

Implementation Date:
This change will be implemented immediately upon approval by the FPKIPA and incorporation into the FBCA CP.

Prerequisites for Adoption:
There are no prerequisites.

Plan to Meet Prerequisites:
There are no prerequisites.

Approval and Coordination Dates:
Date presented to CPWG: April 3, 2008
Date Presented to FPKI PA: July 8, 2008
Date of approval by FPKI PA: July 25, 2008