Federal Bridge CA Certificate Policy Change Proposal
Change Number: 2003-05

To: Federal PKI Policy Authority

From: FPKI Certificate Policy Working Group

Subject: Proposed modifications to the FBCA Certificate Policy

Date: 01 August 2003

Title: FBCA Operational Authority Independent Audit Qualifications.

Version and Date of Certificate Policy Requested to be changed:

X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), dated 10 September 2002.

Change Advocates Contact Information:

Name: Cheryl Jenkins
Organization: GSA
Telephone number: 571-259-9923
E-mail address: cheryl.jenkins@gsa.gov

Organization requesting change: E-Authentication Program Office – FBCA Operational Authority

Change summary: The FBCA OA proposes that the qualifications for the FBCA's independent auditor include knowledge and experience in Public Key technology. Requirements for independent auditors at Entity CAs are not modified, so mapping requirements are not affected.

Background: The FBCA CPWG met on 01 August 2003 to discuss the proposed language and the necessity to broaden the qualifications beyond having knowledge and experience with information technology security requirements.

The following text in italics, underlined, and red font are used to depict specific changes.

Specific Changes:
Specific changes are made to section 2.7.2. Current text is as follows:

> **2.7.2 Identity/Qualifications of Compliance Auditor**
> The auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with requirements which the Federal PKI Policy Authority imposes on the issuance and management of FBCA certificates, and which Entities impose on the issuance and management of their certificates. The compliance auditor must perform such compliance audits as a primary responsibility. The FBCA Operational Authority shall identify the compliance auditor for the FBCA.

Replace with the following text *(changes are shown with italics, underlined, and red text).*

> **2.7.2 Identity/Qualifications of Compliance Auditor**
> The auditor must demonstrate competence in the field of compliance audits. *At the time of the audit, the FBCA compliance auditor*, must be thoroughly familiar with requirements which the Federal PKI Policy Authority imposes on the issuance and management of FBCA certificates. *Likewise, the Entity CA compliance auditor must be thoroughly familiar with the requirements* which Entities impose on the issuance and management of their certificates. The compliance auditor must perform such compliance audits as a primary responsibility.
>
> *For the FBCA, in addition to the previous requirements, the auditor must be a Certified Information System Auditor (CISA), IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.* The FBCA Operational Authority shall identify the compliance auditor for the FBCA.

Estimated Cost:
The cost of procuring auditing services is unchanged, since this reflects the FBCA Operational Authority's current practice and the change does not apply to entity CAs.

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

Prerequisites for Adoption:
There are no prerequisites.

Plan to Meet Prerequisites:
There are no prerequisites.

Approval and Coordination Dates:

Date presented to CPWG:	01 August 2003
Date CPWG recommended approval:	12 August 2003
Date Presented to FPKI PA:	09 September 2003
Date of approval by FPKI PA:	09 September 2003