

# Federal Public Key Infrastructure Policy Authority (FPKIPA)

Minutes of the 09 September 2003 Meeting  
1800 F Street, Room 5141A, Washington, DC

## A. AGENDA

1. Introductions
2. Vote on Approval of Meeting Minutes
3. Federal Identity Credentialing Committee (FICC) Report
4. FBCA Operational Authority (FBCA OA) Report
5. Certificate Policy Working Group (CPWG) Report
6. Other Topics
7. Next Meeting/Meeting Adjourned

## B. VOTING MEMBER ATTENDANCE LIST

- 1) Department of the Treasury – Michelle Moldenhauer
- 2) Department of Commerce – Tim Polk, NIST (proxy)
- 3) Department of Justice – Kevin Deeley
- 4) Department of Defense – Dave Hanko (proxy)
- 5) General Services Administration – David Temoshok
- 6) Office of Management & Budget – Absent
- 7) National Aeronautics and Space Administration – Absent
- 8) National Finance Center – Kathy Sharp (telecon)

## C. MEETING ACTIVITY

### Agenda Items 1 & 2

#### Introductions / Vote on Approval of Meeting Minutes:

Michelle Moldenhauer, Department of the Treasury and current Chair of the FPKIPA, called the meeting to order on 09 September 2003 at 9:40am in Room 5141A of the GSA Building, located at 1800 F Street N.W. in Washington, DC. The FPKIPA did not hold a meeting in August 2003. The meeting minutes for 8 July 2003 were discussed, voted on, and approved by the following FPKIPA members:

Member	Vote
Department of the Treasury	Yes
Department of Defense	Yes
Department of Justice	Yes
National Finance Center/USDA	Yes
Department of Commerce	Yes (Proxy by Tim Polk)
NASA	Abstain
GSA	Yes
OMB	Yes (Proxy by FPKIPA Chair)

The FPKIPA/FICC Webmaster will post the approved 8 July 2003 meeting minutes to the FPKIPA web site.

### **Agenda Item 3**

#### **Federal Identity Credentialing Committee Report (FICC) - Judy Spencer**

The new Common Policy is close to completion with only one outstanding change needed from Tim Polk.

The FICC has a meeting scheduled for next Friday (19 September 2003) with voting members (50) and the at-large group expected to be present.

The Smart Card policy is still being developed, based on the v2.1 NIST standard. The Smart Card Interoperability Program is due by 15 September, but it still needs identity assurance requirements. Standardization is not the issue, but identity proofing is the issue when accepting credentials from other agencies.

In a recent meeting with Tim Polk, NIST, an architectural proposal was developed for the Federal PKI solution being explored by the Federal Identity Credentialing Committee. Ms. Spencer, FICC Chair, drew and explained a diagram of this architectural proposal on the white board. This architecture is designed around the idea of a new PKI with both the FBCA and Federal Common Policy framework working with a Root Authority, a Citizens & Commerce Cert CA, and a Federal Trusted Root Authority. To bring all these components together in a Federal Trust Anchor design will require the FBCA, Common Policy and C4 CAs to have a one way cross certificate. All of this could be part of the FBCA membrane. The FBCA will maintain external relationship entities with their own CAs. The Federal Common Policy CA will establish relationships with shared service providers.

**ACTION (58) – Distribute new FICC-proposed Federal PKI architecture and design work to the FBCA TWG and arrange a meeting for further discussion and recommendations. (Cheryl Jenkins, GSA)**

The Office of the Federal Registry (OFR) needs help from Treasury and NFC to help applications discover certificate paths. NFC is currently working on rolling out three applications and will demonstrate these at the NFC Expo on 30 September in Washington, DC.

**ACTION (59) – Contact Kathy Sharp, USDA/NFC, to see who in Treasury is working with NFC to help the Office of the Federal Registry (OFR). (Treasury)**

Managed services for government agencies and others that handle operational issues (RA/LRA) will need to have a vote by the FPKIPA to gain approval as a recognized product or solution that is a viable candidate for cross certification with the FBCA. Then it will need to be investigated how representatives will be designated for these managed services.

Applicants that are currently in the process of pursuing cross certification with the FBCA are: Federal Deposit Insurance Corporation (FDIC), Department of Justice, Department of Labor,

Department of Energy, Department of State, Department of Homeland Security, State of Illinois, Government of Canada, Patent and Trademark Office (PTO), Government Printing Office (GPO), and the ACES vendors. Other governmental agencies will most likely use shared services.

#### **Agenda Item 4**

#### **FBCA Operational Authority (OA) Report – Cheryl Jenkins, FBCA OA Program Manager**

##### **Status of FBCA Certification and Accreditation:**

On 18 July, the FBCA OA met with CIO Counsel to discuss the possibility of conducting a partial risk assessment. This partial C&A would include the new firewall, CA directory, and the ISO online directory. If this partial C&A passes, then a full risk assessment would not be required as all new components to the environment had been tested. The risk assessment for the FBCA operational environment was completed on 12 August, with only minor discrepancies. On 18 August, KPMG witnessed a successful, complete Key Generation Signing Ceremony for the new CA configuration using Windows 2000 operating system servers with the Entrust 6.1 product.

##### **Status of FBCA/Applicant Cross-Certification Technical Testing:**

The FBCA OA provided engineering support to the DOD effort to verify the ability to validate or check the status of end entity certificates with the Department of Defense. This was tested using the Certificate Arbitrator Module (CAM), but some issues related to firewalls and directories were discovered. However, there are still issues surrounding the capability of CAM to handle validation processes. These issues are under engineering investigation. Further end-to-end testing with the Department of Defense can no longer be supported by the FBCA OA.

##### **Government of Canada**

Testing with the Government of Canada for directory interoperability is to be completed 9 September 2003. There is a need to identify an application that can use this cross certification path to enable intra-government communications.

##### **Department of Labor**

Testing is on hold until the Department of Labor provides new contacts to the FBCA OA.

##### **State of Illinois**

The State of Illinois is now having Entrust perform their directory services. The directory support contract is pending and Mark Anderson is the point of contact for the State of Illinois.

##### **Department of Energy**

The Department of Energy has completed directory interoperability testing. Cross certification interoperability testing is to be started soon and their compliance audit should be completed this week.

##### **Department of State**

The Department of State has received the proper documentation for requirements from the FBCA OA and should begin testing with the prototype FBCA within the next couple of weeks.

### **Status of CA Testing:**

It was discovered during prototype testing that key rollover problems exist with the Microsoft, RSA, and Baltimore CA products. All vendors have been contacted and they have responded with proposed solutions. The RSA and Baltimore product solutions have been tested and now satisfy FBCA requirements for interoperability. The FBCA Program manager has requested that a letter from Microsoft about the new added extension in the CRL to meet this requirement be submitted to the FBCA TWG for consideration and eventually submission to the FPKIPA. Key rollover is rarely tested and therefore this nuance is rarely identified during cross certification, and how each vendor addresses this capability is unique.

**ACES** – The FBCA OA is currently waiting for a directory design to be submitted by the ACES Program Manager, Steve Duncan. The architecture is undefined at this time and determinations to make it publicly available or shared is under consideration. An alternative solution is the use of the VeriSign directory and possibly the deployment of LDAP within the FBCA OA will help with this strategy.

FBCA OA plans to buy the RSA and Baltimore CA products by 30 September 2003. Implementation of these new products with the FBCA membrane is to be completed by end of the 2003 calendar year. Also, the FBCA is planning to buy LUNA CA hardware security modules based on the contingency of the product being FIPS certified. The FBCA hot site is schedule to be online by February 2004.

It was announced that the scope of the FBCA OA Engineering team is not to include or conduct end-to-end testing of certificates with applicants for cross certification, but only the CA and certificate processes associated with the proving of interoperability between certificate authorities. This is being implemented as a cost saving issue for the FBCA OA. Instead, FBCA OA development funding allocations will be used to further enhance CAM capabilities for validation purposes.

### **Status on the DOD cross certification certificate**

Originally, the DOD was issued a cross certification certificate from the FBCA in September 2002 for a period of one year. DoD was notified on 18 May 2003 about the upcoming expiration of the FBCA cross certificate, but to date the technical issues impacting continued DoD cross certification with the FBCA haven't been resolved. An extension is being requested by the DOD to address the final issues with completing the full two-way cross certification with the FBCA. It is required of DOD to submit a new MOA to define any new terms and the strategy designed by them to complete this certificate update. Currently, the DOD directory is not available to the FBCA or its cross-certified participants; this has been an outstanding operational issue for the last 4 months. The new directory system hosted by DOD is not known to the FBCA. Mr. Hanko said that Mr. Gil Nolte, Director of the DoD PKI PMO, is actively working on updating the goals and roadmap for the DoD PKI and is planning to present the latest information to the FPKIPA at the 14 October 2003 meeting.

The request for an extension for use of the FBCA cross certification certificate by the DoD PKI while the technical issues are resolved proposal was discussed, voted on, and approved by the

following FPKIPA members (motion for the vote by Tim Polk (Commerce) and seconded by Michelle Moldenhauer (FPKIPA Chair)):

<b>Member</b>	<b>Vote</b>
Department of the Treasury	Yes
Department of Defense	N/A (own proposal)
Department of Justice	Yes
National Finance Center/USDA	Yes
Department of Commerce	Yes (Proxy by Tim Polk)
NASA	Abstain
GSA	Yes
OMB	Yes (Proxy by FPKIPA Chair)

**ACTION (60) – Submit a revised MOA and a proposal for implementation of a new DoD cross certification certificate within 90 days. (Dave Hanko, DoD).**

#### **Agenda Item 5**

**FPKI Certificate Policy Working Group (CPWG) Report:**

At the FPKI CPWG meeting on 3 September 2003 at NIST North, three FBCA CP Change Proposals were discussed and recommended for discussion and approval at an upcoming FPKIPA meeting. The full text of these three change proposals are appended to the end of these minutes. Mr. Polk provided an explanation of the context and content of each of these change proposals. One modification to change proposal 2003-05 was recommended - changing the title of FBCA OA Administrator to read FBCA OA Program Manager. Some additional discussion about the change proposals took place before a single vote was taken to approve and adopt all three change proposals. The motion to vote on these change proposals was made by Tim Polk (Commerce) and seconded by David Hanko (DOD).

**FBCA CP Change Proposals 2003-03, 2003-04, and 2003-05:**

<b>Member</b>	<b>Vote</b>
Department of the Treasury	Yes
Department of Defense	Yes
Department of Justice	Yes
National Finance Center/USDA	Yes
Department of Commerce	Yes (Proxy by Tim Polk)
NASA	Abstain
GSA	Yes
OMB	Yes (Proxy by FPKIPA Chair)

Three upcoming CPWG meetings have been scheduled --- on 16 September at NIST North to discuss the policy mapping matrix for the Department of Energy and on 22 and 23 September at the Booz Allen Hamilton, National Business Parkway facility to continue the process of

improving the FBCA wording and converting the existing FBCA CP to the new RFC 2527 framework. As usual, these meetings are scheduled from 09:30am – 4:30pm.

**ACTION (61) – Incorporate the new FBCA CP Change Proposals (2003-01 through 2003-05) into the FBCA CP, dated 10 September 2002, and forward the resulting FBCA CP to the FPKIPA webmaster for posting to the Federal PKI web sites. (IATAC)**

**ACTION (62) - Define the NIAP certification requirement for future bridge membrane applications. (Tim Polk, NIST)**

### **Agenda Item 6**

#### **Other Topics:**

- Educause has a couple of CP elements that they would like to present at the next CPWG.
- NFC to demonstrate certificate applicability at the USDA South Building located on 14<sup>th</sup> Street NW Washington DC by The Mall, on 19 September 2003.

#### **Review of Action Items:** See table below.

- Action Item 37 is closed – the Criteria and Methodology document allows for both a CP and CPS to be used for policy mapping exercises to meet requirements.

### **Agenda Item 7**

#### **Next Meeting/Meeting Adjourned**

The next FPKIPA meeting is scheduled for 14 October 2003 from 09:30-11:30 at the GSA facility located at 1800 F Street, Room 5141A, Washington, DC.

A motion to adjourn the meeting was made by Michelle Moldenhauer (FPKIPA Chair) and seconded by David Hanko (DoD). The meeting was officially adjourned at 11:45 a.m.

**D. LIST OF ATTENDEES**

<b>NAME</b>	<b>Email</b>	<b>Telephone</b>	<b>Organization</b>
Alterman, Peter	peter.alterman@nih.gov	301.252.8846	HHS
Cornell, John	john.cornell@gsa.gov	202.501.1598	GSA
Davis, Russell	rdavis@fdic.gov	703.516.5107	FDIC
Deeley, Kevin	kevin.deeley@usdoj.gov	202.353.2421	Justice
Dilley, Brian	dilley_brian@bah.com	410.684.6202	IATAC
Faut, Nathan	nfaut@educause.edu	301.335.2656	Educause
Hanko, Dave	djhanko@missi.ncsc.mil	410.854.4900	DoD PKI PMO
Jenkins, Cheryl	cheryl.jenkins@gsa.gov	571.259.9923	GSA/FTS
Lentz, Mark	lentz_mark@bah.com	410.684.6520	IATAC
Lins, Andrew	andrew.lins@mitretek.org	703.610.1786	Mitretek
Marsh, Georgia	georgiak.marsh@gsa.gov		GSA
Moldenhauer, Michelle	michelle.moldenhauer@do.treas.gov	202.622.1110	Treasury
Petrick, Brant	brant.petrick@gsa.gov	202.208.4673	FICC
Polk, Tim	tim.polk@nist.gov	301.975.3348	NIST
Sharp, Kathy	kathy.sharp@usda.gov	504.255.5638	USDA/NFC
Spencer, Judith	judith.spencer@gsa.gov	202.208.6576	FICC
Tate, Darron	darron.tate@mitretek.org	703.610.1905	Mitretek
Temoshok, David	david.temoshok@gsa.gov	202.208.7655	GSA
Timchak, Steve	stephen.timchak@gsa.gov	703.872.8604	GSA

**E. CURRENT ACTION ITEMS**

<b>No.</b>	<b>Action Statement</b>	<b>POC</b>	<b>Start Date</b>	<b>Status</b>
004	<p>Define the audit criteria (Web Methods, SAS70, PAG) that will be used to conduct C&amp;A sessions for the FBCA and FBCA OA.</p> <p>14 January 2003 – This delta report of what is covered by each C&amp;A technique has been deferred until the completion of the FBCA Criteria and Methodology documents.</p>	<p>Tim Polk, CPWG Co-chair</p>	<p>08 April 2002</p> <p>Updated – 14 January 2003</p> <p>Updated – 13 May 2003</p>	<p><b>Open</b> – reassigned to GSA/FTS, Cheryl Jenkins (as of 14 Jan 2003) and Tice DeYoung</p>
023	<p>CPWG Mapping Report of NFC Basic Assurance</p> <p>14 January 2003 – Tim Polk is to finalize this report and delivery it to the FPKIPA for approval.</p>	<p>Tim Polk</p>	<p>25 October 2002</p> <p>Updated – 14 January 2003</p>	<p><b>Closed</b></p>

No.	Action Statement	POC	Start Date	Status
031	MOAs for the Cross Certification applicants; DoD, NASA, Treasury and USDA/NFC need to be sent to the FBCA OA in original format with signatures.	IATAC/ FPKIPA Chair	Updated - 13 May 2003	<b>Open</b>
037	Review the Methodology/Criteria document and confirm that there isn't any text to prohibit the use of an applicant's CP and CPS for policy mapping evaluations.	Judy Spencer, GSA Tim Polk, NIST	Updated - 21 March 2003	<b>Closed</b>
042	Provide Mr. Polk with a business case for adding new members to the FBCA membrane.	Cheryl Jenkins, GSA	13 May 2003	<b>Closed</b>
043	Establish policy to reflect the changing interoperability needs of the multiple membrane members, and forward requested changes to Mr. John Cornell for review before sending out to the working group members.	Tim Polk, NIST	13 May 2003	<b>Open</b>
048	Solicit participants with a real application to do business with Canada.	Judy Spencer, GSA	10 June 2003	<b>Open</b>
049	Determine if VeriSign is going to specify a unique OID for Federal managed clients that are covered under the Delta CP.	CPWG	10 June 2003	<b>Open</b>
050	The State of Illinois MOA should be written to reflect that any changes to their CPS must be forwarded to the FPKIPA and that both the CP and CPS from the State of Illinois were used for the mapping comparison with the FBCA CP.	Tim Polk	10 June 2003	<b>Open</b>
053	Review FBCA CP to address "verified credentials" (FBCA CP, Section X.X.X). This will be done at the upcoming off-site meeting.	CPWG	10 June 2003	<b>Open</b>
054	Develop a cover letter for the Liability Language for CPs (John Cornell, GSA) and then sign it and send it to Dept of Justice (Ms. Moldenhauer, FPKIPA Chair).	John Cornell, GSA Michelle Moldenhauer, Treasury	10 June 2003	<b>Open</b>
057	Write a short paper that says from here forward the FBCA OA will limit	Tim Polk	8 July 2003 Updated – 9 September	<b>Open</b>

No.	Action Statement	POC	Start Date	Status
	FBCA acceptance testing to systems that demonstrate enhanced assurance through NIAP testing.		2003	
058	Distribute new FICC proposed PKI architecture and design work to the FBCA TWG and arrange a meeting for further discussion and recommendations.	Cheryl Jenkins, GSA	9 September 2003	<b>Open</b>
059	Contact Kathy Sharp, USDA/NFC, to see who in Treasury is working with NFC to help the Office of the Federal Registry (OFR).	Treasury	9 September 2003	<b>Open</b>
060	Submit a revised MOA and a proposal for implementation of a new DoD cross certification certificate within 90 days.	Dave Hanko, DoD	9 September 2003	<b>Open</b>
061	Incorporate the new FBCA CP Change Proposals (2003-01 through 2003-05) into the FBCA CP, dated 10 September 2002, and forward the resulting FBCA CP to the FPKIPA webmaster for posting to the Federal PKI web sites.	IATAC	9 September 2003	<b>Open</b>
062	Define the NIAP certification requirement for future bridge membrane applications.	Tim Polk, NIST	9 September 2003	<b>Open</b>



**Federal Bridge CA Certificate Policy Change Proposal**  
**Change Number: 2003-03**

**To:** Federal PKI Policy Authority  
**From:** FPKIPA Certificate Policy Working Group  
**Subject:** Proposed modifications to the FBCA Certificate Policy  
**Date:** 9 September 2003  
**Title:** FBCA Event Logging

**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: Tim Polk  
Organization: NIST  
Telephone number: 301-975-3348  
E-mail address: tim.polk@nist.gov

**Organization requesting change:** Federal PKI Policy Authority – Certificate Policy Working Group

**Change summary:** The FPKIPA CPWG proposes clarifying the requirements stated in Section 4.5 qualifications with respect to messages requesting action by the CA. In addition, this change proposal removes references to the MOA for Test Assurance level and the CIMC Protection Profile.

**Background:** The FBCA CPWG meeting with the ACES Program Manager, Steve Duncan, on 30 May 2003 that discussed the Generic and Medium policy mapping requirements of the ACES certificate policy to the FBCA CP. This proposed language eliminates a restriction placed on Entity CAs that is unenforceable by the FPKIPA or FBCA OA.

**Specific Changes:**

Specific changes are made to FBCA Section 4.5.1

*A message from any source received by the FBCA or Entity CA 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 when executing the FBCA signing process.
- A success or failure indicator when performing certificate revocation.
- The identity of the entity and/or operator (of the FBCA) that caused the event.

*Detailed audit requirements are listed in the table below.* All security auditing capabilities of the FBCA or Entity CA operating system and PKI CA applications required by this CP shall be enabled. As a result, most of the events identified in the table shall be automatically recorded.

**Estimated Cost:**

The cost of this change to the FBCA CP in nominal, as cost is associated with the editing, publishing and distribution of the new certificate policy. There is no cost associated with operations or maintenance of the FBCA for 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: **3 September 2003**

Date CPWG recommended approval: **3 September 2003**

Date Presented to FPKI PA: **9 September 2003**

Date of approval by FPKI PA: **9 September 2003**



**Federal Bridge CA Certificate Policy Change Proposal**  
**Change Number: 2003-04**

**To:** Federal PKI Policy Authority  
**From:** FPKIPA Certificate Policy Working Group  
**Subject:** Proposed modifications to the FBCA Certificate Policy  
**Date:** 9 September 2003  
**Title:** FBCA Token Destruction

**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: Tim Polk  
Organization: NIST  
Telephone number: 301-975-3348  
E-mail address: tim.polk@nist.gov

**Organization requesting change:** Federal PKI Policy Authority – Certificate Policy Working Group

**Change summary:** The FPKIPA CPWG proposes that the requirement stated in Section 4.4.1.2 for the destruction or zeroization of tokens be modified to address issues of the Certification Authority not having ownership of the device.

**Background:** The FBCA CPWG meeting with the State of Illinois, Georgia Marsh, on 4 April 2003 that discussed the Generic and Medium policy mapping requirements of the State of Illinois certificate policy to the FBCA CP. This proposed language eliminates a restriction placed on Entity CAs that is unenforceable by the FPKIPA or FBCA OA.

**Specific Changes:**

Replace paragraph four of FBCA CP Section 4.4.1.2:

For PKI implementations using hardware tokens, a Subscriber ceasing its relationship with an organization that sponsored the certificate shall, prior to departure, surrender to the organization (through any accountable mechanism) all cryptographic hardware tokens that were issued by or on behalf of the sponsoring organization. If a Subscriber leaves an organization and the hardware tokens cannot be obtained from the Subscriber, then all Subscribers' certificates associated with the unretrieved tokens shall be immediately revoked. The token shall be zeroized or destroyed promptly upon surrender and shall be protected from malicious use between surrender and zeroization or destruction.

with the following text:

For PKI implementations using hardware tokens, revocation is optional if all the following conditions are met:

- The revocation request was not for key compromise;
- The hardware token does not permit the user to export the signature private key;
- The Subscriber surrendered the token to the PKI;
- The token was zeroized or destroyed promptly upon surrender;
- The token has been protected from malicious use between surrender and zeroization or destruction.

In all other cases, revocation of the certificates is mandatory. Even where hardware tokens are zeroized or destroyed, revocation of the associated certificates is recommended.

**Estimated Cost:**

The cost of this change to the FBCA CP is nominal, as cost is associated only with the editing, publishing and distribution of the new certificate policy. There is no cost associated with operations or maintenance of the FBCA for 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: **3 September 2003**

Date CPWG recommended approval: **3 September 2003**

Date Presented to FPKI PA: **9 September 2003**

Date of approval by FPKI PA: **9 September 2003**



**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:** 9 September 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.

**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 (*inserted text in italics*):

### **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 Administrator shall identify the compliance auditor for the FBCA.*

#### **Estimated Cost:**

The cost of procuring auditing services for the FBCA is unchanged, since this reflects the FBCA Operational Authority's current practice. The cost of procuring auditing services for each entity cross certifying with the FBCA is not affected, since the change does not apply to entity CAs.

#### **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:	<b>3 September 2003</b>
Date CPWG recommended approval:	<b>3 September 2003</b>
Date Presented to FPKI PA:	<b>9 September 2003</b>
Date of approval by FPKI PA:	<b>9 September 2003</b>