

Federal Public Key Infrastructure Policy Authority (FPKIPA)

Minutes of the 10 June 2003 Meeting
1800 F Street, Room 5141A, Washington, DC

A. AGENDA

- 1) Introductions
- 2) Vote on Approval of Meeting Minutes
- 3) Federal PKI Steering Committee (FPKI SC) 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 – Proxy by Tim Polk, NIST
- 3) Department of Justice (DoJ) – Absent
- 4) Department of Defense (DoD) – Absent
- 5) General Services Administration (GSA) – David Temoshok
- 6) Office of Management & Budget (OMB) – Absent
- 7) National Aeronautics and Space Administration (NASA) – Tice DeYoung
- 8) National Finance Center (USDA/NFC) – Kathy Sharp

C. MEETING ACTIVITY

Agenda Items 1 & 2

Introductions / Vote on Approval of Meeting Minutes

Ms. Michelle Moldenhauer, FPKIPA Chair, called the meeting to order on 10 June 2003 at 9:48am in Room 5141A of the GSA Building located at 1800 F Street N.W. in Washington, DC.

The meeting minutes for 13 May 2003 were briefly discussed and unanimously approved according to the following vote record:

Approval vote for 13 May 2003 Meeting Minutes			
Voting members	Vote		
	Yes	No	Abstain
Dept of the Treasury	X		
Dept of Commerce	X		
Dept of Justice (proxy by FPKIPA Chair)	X		
Dept of Defense (proxy by FPKIPA Chair)	X		
GSA	X		
OMB (proxy by FPKIPA Chair)	X		
NASA	X		
NFC	X		

Mr. Russ Davis, FDIC, attended the meeting for the first time and introduced himself.

Agenda Item 3

Federal PKI Steering Committee Report

Ms. Judy Spencer discussed the latest developments in the upcoming organizational changes to the current Federal Public Key Infrastructure Steering Committee (FPKI SC). The new group will most likely be renamed as the Federal Identity and Credentialing Committee (FICC). There is a kick-off meeting scheduled for 25 June 2003.

New goals and policy requirements for the FICC were discussed. Ms. Spencer noted that identity proofing is not a new concept, referring to Executive Order 10450, dated 27 April 1953. It specified what OPM does when hiring Federal employees, but it does not apply to executive service and contractors.

Other topics discussed included the requirement for all individuals to have a NAC to prove that they do not have a criminal background. Also discussed was what a person does to become classified as a Federal Government employee.

The Economy Act Order, which allows/specifies the sharing of funds between government departments/agencies for a common mission, is currently at OMB in the rewrite process. This document will provide specific details about the FICC initiative as well as solicit participation.

What is meant by, “establishing the FICC by November 2003”? The FICC is to have a set of policies/budget guidelines for the government agencies and a set of requirements for common credential & service providers in place by mid November 2003. A near-term goal of the FICC is to establish a means of providing physical and logical credentials and PKI for those that need PKI.

Will the Common Criteria be part of the requirements levied on the common service providers? That hasn't been determined yet.

Agenda Item 4

FBCA Operational Authority (OA) Report

Status of FBCA Certification & Accreditation:

The self-assessment for FISMA was completed and forwarded to the CIO of FTS.

The FBCA OA has submitted the necessary documentation to the PKI and information security audit team at KPMG for the Certification & Accreditation (C&A).

The FBCA OA is procuring directory and Certificate Authority (CA) hardware and software for the Production FBCA and its hot-site. The SureWare Keyper Hardware Security Module (HSM) -- a hardware-based security device that generates, stores and protects cryptographic keys, has been tested; however, it does not meet the FBCA OA operational requirements. Therefore, the Luna HSM will be used.

Hardware and software for the Production FBCA and its hot-site are to be installed between 23 June 2003 and 11 July 2003.

Disaster recovery testing will be conducted on 16 July 2003 to: 1) ensure that the FBCA disaster recovery plan minimizes the duration of a serious disruption to the FBCA OA operations; 2) facilitate effective co-ordination of recovery tasks; and 3) reduce the complexity of the recovery effort.

Mitretek will perform a risk assessment on the Production FBCA on 21 July 2003. Mitretek risk assessment team (independent from the FBCA OA team) did the last risk assessment on 21 December 2001.

Status of FBCA/Applicant Cross-Certification Technical Testing

Illinois – Testing will begin once Illinois employ contract support for directory services.

Government of Canada (GoC) – Technical and directory interoperability testing is completed with the GOC's Phase 1 system, which is their test environment. Testing is scheduled with their Phase 2 system -- interim environment. The GOC and the FBCA OA have agreed to 31 August 2003 as the deadline to test with the GOC's Phase 3 system -- Production environment. Although the ISODE will be installed as the FBCA new directory, the FBCA OA is currently testing with the ISO/Peer Logic because it is accredited to operate.

ACTION (48): Ms. Spencer will solicit participants with a real application to do business with Canada

Department of Labor (DoL) – Testing has not been coordinated yet.

Status of CA testing

Microsoft: They completed and passed all requirements for Windows 2000 server/product and directory interoperability.

ACES:

- **Digital Signature Trust:** Cross-certification testing is complete and directory testing is currently ongoing.
- **AT&T:** The FBCA OA is waiting on a reply in order to complete testing.
- **ORC:** The FBCA OA is waiting on a reply in order to complete testing.

Agenda Item 5

Certificate Policy Working Group (CPWG) Report

VeriSign: Discussion of the VeriSign comparison mapping should be complete at the 20 June CPWG meeting. VeriSign is to create a Delta CP with Class 2 OIDs. It was suggested that VeriSign assign a new OID for any Federal managed clients that are covered under the Delta CP.

VeriSign intends to submit the Delta CP after CPWG finishes the review of the mapping and an agreement is made of the necessary VeriSign CP changes.

ACTION (49): The CPWG will determine if VeriSign is going to specify a unique OID for Federal managed clients that are covered under the Delta CP.

DoL – DoL submitted a final CP to FPKI PA on 13 May 2003. It was given to IATAC on 10 June 2003 to conduct a follow-on mapping comparison.

GoC – CPWG representatives attended an on-site meeting at the Canadian facility on 4-5 June 2003. The meeting was productive and the CP mapping comparison is almost complete.

Illinois – The Certificate Policy mapping report was discussed and approved with a few minor corrections at the 6 June CPWG meeting. Here is the voting record:

Approval vote for the State of Illinois CP Mapping Report				
Motion	Voting members	Vote		
		Yes	No	Abstain
2 nd	Dept of the Treasury	X		
1 st	Dept of Commerce	X		
	Dept of Justice (proxy by FPKIPA Chair)	X		
	Dept of Defense (proxy by FPKIPA Chair)	X		
	GSA	X		
	OMB (proxy by FPKIPA Chair)	X		
	NASA			X
	NFC	X		

ACTION (50): 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.

ACTION (51): The “Concerns” section will be removed from the final version of the State of Illinois Mapping Report.

ACES – The ACES mapping report needs to include details of the 30 May CPWG meeting and the correct mapping recommendation of each ACES certificate from the 6 June CPWG meeting.

Mr. Temoshok, GSA, lead a discussion of the Individual Unaffiliated identity certificate process for ACES. During the online registration process, the identity of an Unaffiliated individual is validated online against multiple databases and then the password is delivered to the individual’s physical address. Mr. Temoshok asserted that validating identity against multiple databases, without face-to-face authentication, was comparable to the Medium level of assurance in the FBCA CP. Therefore, GSA recommended that the ACES Mapping Report be changed to reflect that all the certificates in the ACES CP be mapped to the FBCA CP at the Medium level.

Here is the vote record:

Vote for the ACES Mapping Report to specify all ACES Certificates map to the FBCA CP at the Medium level of Assurance				
Motion	Voting members	Vote		
		Yes	No	Abstain
	Dept of the Treasury		X	
	Dept of Commerce		X	
	Dept of Justice (proxy by FPKIPA Chair)		X	
	Dept of Defense (proxy by FPKIPA Chair)		X	
1 st	GSA	Cannot vote on this issue		
	OMB (proxy by FPKIPA Chair)		X	
2 nd	NASA	X		
	NFC		X	

Therefore, as a result of this vote, this motion to overturn the original CPWG recommendation for mapping of the ACES certificates was not passed.

The next step was a recommendation for the ACES Mapping Report to be worded to have the Unaffiliated Individual certificates mapped at the Basic level and the other certificates at the Medium level.

Vote for the ACES Mapping Report to specify the Unaffiliated Individual Certificate at the Basic level of assurance and all other ACES Certificates at the Medium level of Assurance compared to the FBCA CP				
Motion	Voting members	Vote		
		Yes	No	Abstain
	Dept of the Treasury	X		
2 nd	Dept of Commerce	X		
	Dept of Justice (proxy by FPKIPA Chair)	X		
	Dept of Defense (proxy by FPKIPA Chair)	X		
1 st	GSA	Cannot vote on this issue		
	OMB (proxy by FPKIPA Chair)	X		
	NASA		X	
	NFC	X		

As a result of this vote, the recommendation for the mapping levels to be correctly indicated in Mapping Report prior to soliciting an electronic vote as Unaffiliated individual certificates at the Basic level of assurance and the Secure Socket Layer (SSL) server, Business, and Federal government certificates at the Medium level of assurance was passed - 6 to 1.

ACTION (52): The details of the 30 May CPWG meeting and the correct recommendations for mapping each ACES certificate will be corrected in the ACES mapping report prior to its distribution to the FPKIPA voting members for electronic vote.

ACTION (53): CPWG should review fixing FBCA CP to address “verified credentials”. This will be done at the upcoming off- site meeting.

Agenda Item 6

Other Topics

Discussion/Approval of Liability Language for CPs

Finalization of the wording of the Liability Language for CPs is waiting for an opinion from the Department of Justice (DoJ). The Department of Treasury lawyer has reviewed and accepted the new language. DoD wants DoJ to review the language. A vote was taken to formally forward the Liability Language to DoJ for review and comment.

Here is the vote record:

Vote to forward the Liability Language for CPs to the Dept of Justice for review and comment				
Motion	Voting members	Vote		
		Yes	No	Abstain
	Dept of the Treasury	X		
	Dept of Commerce	X		
	Dept of Justice (proxy by FPKIPA Chair)	X		
	Dept of Defense (proxy by FPKIPA Chair)	X		
1 st	GSA	X		
	OMB (proxy by FPKIPA Chair)	X		
2 nd	NASA	X		
	NFC	X		

ACTION (54): John Cornell, GSA, will develop a cover letter for the Liability Language for CPs and Ms. Moldenhauer, FPKIPA Chair, will sign it and send it to Dept of Justice.

Discussion/Approval of MOA Templates

There was some brief discussion on these templates before a vote was recommended.

Vote to approve the MOA Templates				
Motion	Voting members	Vote		
		Yes	No	Abstain
	Dept of the Treasury	X		
1 st	Dept of Commerce	X		
	Dept of Justice (proxy by FPKIPA Chair)	X		
	Dept of Defense (proxy by FPKIPA Chair)	X		
	GSA	X		
	OMB (proxy by FPKIPA Chair)	X		
2 nd	NASA	X		
	NFC	X		

ACTION (55): Mr. McDowell to send the final version of the MOA Templates to Brant Petrick for posting to the FPKIPA web site.

Review of Action Items: The status of the existing action items was briefly discussed, resulting in the revision of some of the action items. Please see the updated Action Item table at the end of these meeting minutes.

Agenda Item 7

Next Meeting/Meeting Adjourned

The next FPKI PA Meeting is scheduled for 8 July 2003 starting at 9:30 am at the GSA Central Office, 1800 F Street NW, Room 5141A, Washington, DC 20405.

D. LIST OF ATTENDEES

NAME	Email	Telephone	Organization
Alterman, Peter	peter.alterman@nih.gov	301.252.8846	FPKISC
Burr, Bill	william.burr@nist.gov	301.975.2914	NIST
Cornell, John	john.cornell@gsa.gov	202.501.1598	GSA
Davis, Russ	rdavis@fdic.gov	703.516.5107	FDIC
DeYoung, Tice	tice.f.deyoung@nasa.gov	703.872.8615	NASA
Dilley, Brian	dilley_brian@bah.com	410.684.6202	IATAC
Faut, Nathan	nfaut@educause.edu	301.335.2656	HEBCA
Harrison, Von	von.harrison@gsa.gov	202.273.0721	GSA
Lentz, Mark	lentz_mark@bah.com	410.684.6520	IATAC
McDowell, Gene	eugene.c.mcdowell@noaa.gov	301.713.3333 x207	NOAA
Moldenhauer, Michelle	michelle.moldenhauer@do.treas.gov	202.622.1110	Treasury
Petrick, Brant	brant.petrick@gsa.gov	202.208.4673	FPKISC
Polk, Tim	tim.polk@nist.gov	301.975.3348	NIST
Sharp, Kathy (telecon)	kathy.sharp@usda.gov	504.255.5638	USDA/NFC
Spencer, Judith	judith.spencer@gsa.gov	202.208.6576	FPKISC
Tate, Darron	darron.tate@mitretek.org	703.610.1905	MTS
Temoshok, David	david.temoshok@gsa.gov	202.208.7655	GSA

E. CURRENT ACTION ITEMS

No.	Action Statement	POC	Start Date	Status
004	<p>Define the audit criteria (Web Methods, SAS70, PAG) that will be used to conduct C&A sessions for the FBCA and FBCA OA.</p> <p>14 January 2003 – This delta report of what is covered by each C&A technique has been deferred until the completion of the FBCA Criteria and Methodology documents.</p>	<p>Tice DeYoung, NASA</p>	<p>08 April 2002</p> <p>Updated – 14 January 2003</p> <p>Updated – 13 May 2003</p>	<p>Open – reassigned to Cheryl Jenkins (14 Jan 2003) and Tice DeYoung (13 May 2003)</p>

No.	Action Statement	POC	Start Date	Status
023	CPWG Mapping Report of NFC Basic Assurance 14 January 2003 – Tim Polk is to finalize this report and delivery it to the FPKIPA for approval.	IATAC	25 October 2002 Updated – 14 January 2003	Open
030	Define the Security target used in Common Criteria (CC) testing.	Tim Polk	14 January 2003	Closed
031	MOA's 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	14 January 2003	Open
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	21 March 2003	Open
041	Send an email to the FPKI PA working group members with the proposed FBCA CPS language on identity proofing requirements.	Cheryl Jenkins, GSA	13 May 2003	Closed
042	Provide Mr. Polk with a business case for adding new members to the FBCA membrane.	Cheryl Jenkins, GSA	13 May 2003	Open
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	Open
044	Submit comments on the Common Policy CP to Mr. Polk before 30 May.	FPKIPA members	13 May 2003	Closed
045	Develop/distribute outstanding FBCA CP change proposals and set up a special focus FPKI CPWG meeting in September 2003 to discuss and approve them.	Tim Polk, NIST and IATAC	13 May 2003	Open
046	Distribute the FBCA CP in the new RFC 2527 format.	IATAC	13 May 2003	Closed
048	Solicit participants with a real application to do business with Canada.	Judy Spencer, GSA	10 June 2003	Open
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	Open

No.	Action Statement	POC	Start Date	Status
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	Open
051	Remove “Concerns” section from the Illinois Mapping Report.	IATAC	10 June 2003	Closed
052	Correct the ACES mapping report with the details of the 30 May CPWG meeting and the correct recommendations for mapping each ACES certificate prior to its distribution to the FPKIPA voting members for electronic vote.	IATAC	10 June 2003	Closed
053	Review FBCA CP to address “verified credentials”. This will be done at the upcoming off-site meeting.	CPWG	10 June 2003	Open
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	Open
055	Submit the MOA Templates to Brant Petrick for posting to the FPKIPA web site.	Gene McDowell	10 June 2003	Closed