

Federal Public Key Infrastructure Policy Authority (FPKIPA)

Minutes of the 13 May 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 – Absent
- 4) Department of Defense (DoD) – Gil Nolte
- 5) General Services Administration – David Temoshok
- 6) Office of Management & Budget (OMB) – Jeanette Thornton
- 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, Department of the Treasury, called the meeting to order on 13 May 2003 at 9:40am in Room 5141A of the GSA Building located at 1800 F Street N.W. in Washington, DC.

The meeting minutes for December 2002 and March 2003 were discussed, voted, and approved by OMB (by proxy), Treasury, Justice (by proxy), Commerce, DoD, GSA, NASA, and NFC. Mr. Brant Petrick will post these approved minutes on the FPKIPA web site.

It was suggested that in the future when an electronic vote is sent to the group that the word “VOTE” be used at the beginning of the subject line of the email message. Also, if votes are not received by the deadline specified in the message, it should be assumed that the organization will have no comments and is in favor of its approval, by default.

Mr. Gil Nolte, Mr. Mike Green's successor, as the DoD PKI PMO Director, attended this FPKI PA meeting for the first time.

Agenda Item 3

Federal PKI Steering Committee Report

Ms. Judy Spencer discussed the upcoming change in the mission and organization of what is currently known as the Federal Public Key Infrastructure Steering Committee (FPKI SC). The new group, in addition to maintaining its ties to the future of the FPKI, will also oversee the migration to the common services such as the Federal ID credentials to include the integration of logical and physical controls. Due to the re-organization, the Common Policy Framework will be added to the list of responsibilities of the group. Digital signatures are to be issued under this Common Policy Framework. This new group will result from the merging or integrating of current Smart Card, PKI, HR, and Physical Security groups to meet new group objectives and should be fully operational in the fall of 2003.

As a result of its new focus, the FPKI SC will be renamed, with the leading choice so far being the "Federal Identity Management Committee". This suggested name has not been confirmed at this time.

The e-Authentication Steering Committee was also recently formed and consists of 15 member organizations to include; Department of Defense (DoD), Department of Labor (DoL), Department of Commerce, Department of Energy (DoE), General Services Administration (GSA), National Aeronautical and Space Administration (NASA), Social Security Administration (SSA), Department of Housing and Urban Development (HUD), Department of Health and Human Services (HHS), Veterans Administration (VA,) Department of the Treasury, Environmental Protection Agency (EPA), Department of State, United States Department of Agriculture (USDA), and the Department of Education. Each of these 15 member organizations has been asked to identify a primary and alternate point of contact for this subgroup. Mr. Drew Ladner, the new Treasury CIO, was nominated and has accepted the role of Chair of the e-Authentication Steering Committee for the first year. The next meeting is scheduled for 5 June 2003.

Action Item #040 - Ms. Spencer will forward the official version of the slides pertaining to the OMB e-Authentication Policy to the FPKI PA members.

Agenda Item 4

FBCA Operational Authority (OA) Report

Status of FBCA Certification & Accreditation:

On 2 May FBCA received an extension to the interim authorization to operate. The extension included 24x7 operational support, establishment of the FBCA OA "hot site", archive requirements, and architectural changes. OMB needs a Full Authorization to Operate (FATO) due to IATO parameters not being consistent between Agencies. The FBCA OA is in the process of doing paperwork before the start of the ST&E and Risk Assessment, purchasing

hardware and software for the new architecture, and is on target to become fully operational by the end of 2003.

The FBCA OA had a successful testing on the ISODE directory. Luna made an offer to let the FBCA borrow HSM equipment until the new equipment becomes available. The FBCA OA is waiting on the decision to be made on which HSMs to use.

Identity Proofing - Prior to the cross certifying entities in September 2002, the FBCA OA did not have to validate ID's. The Government of Canada (GoC) and the State of Illinois will require ID validation. This can possibly be accomplished under the ACES program. The FBCA CPS needs to be reviewed to verify if new validation procedures (in person proofing) will need to be changed. This will be discussed further in the 30 May 2003 CPWG Meeting. The CPWG will review Canada's proofing process at the 5 June 2003 meeting.

Action Item #041 - Ms. Jenkins will send an email to the FPKI PA working group members with the proposed FBCA CPS language on identity proofing requirements.

List Servers - The CPWG, PA and FBCA TWG list servers are already established, but not currently being used. Mr. Tice DeYoung proposed that the lists be maintained and we start using them. Mr. Polk 2nd the motion and OMB, Treasury, GSA, DoD, NASA, Commerce, NFC, and Justice (by proxy) all agreed that Mitretek is to maintain the CPWG, PA, and FBCA TWG list servers and associated mail lists.

Status of FBCA/Applicant Cross-Certification Technical Testing:

Current:

DoD (KMI): Technical interoperability testing has been completed. Parsing of certificate extensions was acceptable, although extra extensions were not recognized, so the DoD will retest and fix any remaining errors.

State of Illinois: They still need support for their directory.

Government of Canada: Tested trust with FBCA last week. Reverse testing completed including directory testing.

Future:

Department of Labor: The FBCA should be contacted to coordinate testing soon.

Department of State: The FBCA has done the high level mapping, and Department of State will need to formally submit their CP and the compliance audit report in order to proceed.

Status of CA testing

Current:

Microsoft: They are reviewing test plans before moving forward with the testing, but the FBCA OA envisions that the testing will go quickly since a beta test was already done.

Future:

ACES: The Policy Mapping is scheduled to be reviewed at the 30 May 2003 CPWG meeting. Ms Jenkins requested that the testing be completed by 30 May 2003 so that they can keep on schedule to complete ACES by 15 June 2003. There is a meeting tentatively scheduled for 6 June 2003 at 1300 at NIST to meet with the ACES vendors in order to complete the process by 15 June 2003.

FBCA OA is trying to get all the known testing done by 30 May 2003.

Ms Jenkins posed the question concerning limiting the FBCA membrane to the 4 that are already in the FBCA prototype (Baltimore, RSA, Entrust and Microsoft).

Action Item #042 - Ms. Jenkins will provide Mr. Polk with a business case for adding new members to the FBCA membrane.

Action Item #043 - Mr. Polk will 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 and posting to the FBCA web site.

Agenda Item 5

FPKI Certificate Policy Working Group (CPWG) Report

The DoL policy mapping is complete and a CPWG Meeting was held on 8 May 2003. DoL is working on their revised CP, and they have yet to do their compliance audit.

VeriSign: Proposing an addendum to their CP for Federal Government customers to choose implementation options that meet the FBCA CP at the Medium Assurance Level.

Common Policy CP: All comments that have been made to the Common Policy CP have been addressed to date. Additional comments need to be sent to Mr. Polk before 30 May. The FBCA CP will incorporate the new guidelines for key strength (2048 bits with SHA256).

Action Item #044 - The revised Common Policy CP was distributed to the FPKIPA members on 12 May 2003 and comments are due back to Mr. Tim Polk by 30 May to prepare for CIO Council review on 15 June 2003.

Action Item #045 - The outstanding FBCA CP change proposals will be distributed and a special focus FPKI CPWG meeting held in June 2003 to discuss and approve them.

Action Item #046 - Distribute the FBCA CP in the new RFC 2527 format, as soon as the reformatting process is done by IATAC.

Agenda Item 6

Other Topics

Discussion/Approval of Liability Language for Federal Agency CPs: Treasury and DoD would like to have their lawyers review the document first. A vote will be conducted at the June FPKI PA Meeting. Please send any comments/questions to Mr. Gene McDowell.

Action Item #047 - Add the topic of “Vote for Approval of Liability Language for Federal Agency CPs” to the agenda for the 10 June 2003 FPKI PA Meeting.

Discussion/Approval of MOA Templates: Mr. McDowell explained the differences between the MOAs in the one page document entitled, “Dispute Resolution Language for MOAs with Federal and Non-Federal Entities”. The templates are all identical except for these dispute resolution sections. Ms. Moldenhauer suggested that each FPKI PA voting member lawyer review these templates and get comments to Mr. McDowell.

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 10 June 2003 from 9:30 a.m. to 12:00 p.m. at the General Services Administration (GSA) Central Office, 1800 F Street, NW (Room # 5141A) Washington, DC 20405.

This meeting adjourned at 11:55am.

D. LIST OF ATTENDEES

NAME	Email	Telephone	Organization
Alterman, Peter	peter.alterman@nih.gov	301.252.8846	FPKISC
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	301.665.2656	Educause
Hanko, Dave	djhanko@missi.ncsc.mil	410.854.4900	DoD PKI PMO
Jenkins, Cheryl	cheryl.jenkins@gsa.gov	202.345.4096	GSA
Lentz, Mark	lentz_mark@bah.com	410.684.6520	IATAC
Lins, Andrew	andrew.lins@mitretek.org	703.610.1786	Mitretek Systems (MTS)
McDowell, Gene	eugene.c.mcdowell@noaa.gov	301.713.3333 x207	NOAA
Moldenhauer, Michelle	michelle.moldenhauer@do.treas.gov	202.622.1110	Treasury
Nolte, Gil	gnolte@missi.ncsc.mil	410.854.4900	DoD PKI PMO
Patterson, Shelly	patterson_shelly@bah.com	410.684.6478	IATAC
Petrick, Brant	brant.petrick@gsa.gov	202.208.4673	FPKISC
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	FPKISC
Tate, Darron	darron.tate@mitretek.org	703.610.1905	Mitretek Systems (MTS)
Thornton, Jeanette	jthornto@omb.eop.gov	202.395.3562	OMB

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>	Tice DeYoung, NASA	<p>08 April 2002</p> <p>Updated – 14 January 2003</p> <p>Updated – 13 May 2003</p>	Open – reassigned to Cheryl Jenkins (14 Jan 2003) and Tice DeYoung (13 May 2003)
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>	Tim Polk	<p>25 October 2002</p> <p>Updated – 14 January 2003</p>	Open
030	<p>NIST to define the Security target used in Common Criteria (CC) testing.</p>	Tim Polk	14 January 2003	Closed

No.	Action Statement	POC	Start Date	Status
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
032	It was requested by the FBCA OA to provide the FPKIPA Meeting Minutes that show voting approval for each cross certification applicant and the CPWG report of the Mapping Matrix be included as part of the FBCA Cross Certification Package	IATAC	14 January 2003	Closed
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
040	Forward the official version of the slides pertaining to the OMB e-Authentication Policy to the FPKI PA members.	Judy Spencer, GSA	13 May 2003	Closed
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	Open
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 and posting to the FBCA web site.	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 June 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	Open
047	Add the topic of "Vote for Approval of Liability Language for Federal Agency CPs" to the agenda for the 10 June 2003 FPKI PA Meeting.	IATAC	13 May 2003	Closed