

Federal Public Key Infrastructure Policy Authority (FPKIPA)

Minutes of the 11 May 2004 Meeting

GSA; 1800 F Street; Room 5141B; Washington, DC

A. AGENDA

- 1) Introductions
- 2) Approval Vote on Minutes from 9 March 2004
- 3) Status of Email Votes Since Last FPKIPA Meeting
- 4) Vote on Updated FPKIPA Charter, Version 1.4
- 5) PKI Implementation Issues from DoD and NASA
- 6) Federal Identity Credentialing Committee (FICC) Report
- 7) FPKI Certificate Policy Working Group (FPKI CPWG) Report
- 8) FBCA Operational Authority (FBCA OA) Report
- 9) Other Topics
- 10) Next Meeting Plans / 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 – Proxy by Dave Hanko
- 5) General Services Administration – Proxy by John Cornell
- 6) Office of Management & Budget – Absent
- 7) National Aeronautics and Space Administration – Tice DeYoung
- 8) National Finance Center – Absent

C. MEETING ACTIVITY

Agenda Items 1 & 2

Introductions / Vote on Approval of Meeting Minutes:

Ms. Michelle Moldenhauer, Chair of the FPKIPA, called the meeting to order at 9:40 a.m. with attendee introductions.

Regarding the 9 March 2004 FPKIPA meeting minutes, only editorial comments were mentioned and later shared with IATAC after the meeting. Here is the voting record:

Approval vote for 10 February 2004 FPKIPA Meeting Minutes			
Voting members	Vote (Motion – NASA; 2 nd – DoD)		
	Yes	No	Abstain
Dept of the Treasury	X		
Dept of Commerce	X		
Dept of Justice (proxy by FPKIPA Chair)	X		
Dept of Defense	X		
GSA	X		
OMB (proxy by FPKIPA Chair)	X		
NASA	X		
NFC (proxy by FPKIPA Chair)	X		

Agenda Item 3

Status of Email Votes Since Last FPKIPA Meeting:

There were no email votes conducted since the last FPKIPA meeting on 9 March 2004.

Agenda Item 4

Vote on Updated FPKIPA Charter, Version 1.4:

Recent review of the FPKIPA Charter, Version 1.3, that was approved by the FPKIPA in February 2004, revealed that some text was inadvertently omitted from Section 6. More specifically, in both Section 6.1 (a) and Section 6.2, the following phrase should be the correct text, "...FBCA Certificate Policy or the X.509 Certificate Policy for the Common Policy Framework". None of the attendees objected to correcting the text in the referenced locations in the FPKIPA Charter. Here is the voting record:

Approval vote for FPKIPA Charter, Version 1.4			
Voting members	Vote (Motion – NASA; 2 nd – Commerce)		
	Yes	No	Abstain
Dept of the Treasury	X		
Dept of Commerce	X		
Dept of Justice (proxy by FPKIPA Chair)	X		
Dept of Defense	X		
GSA	X		
OMB (proxy by FPKIPA Chair)	X		
NASA	X		
NFC (proxy by FPKIPA Chair)	X		

Agenda Item 5

PKI Implementation Issues from DoD and NASA

Since the 9 March FPKIPA meeting, DoD and NASA have forwarded four technical issues to the FPKIPA mail list for awareness, consideration and input. Here are the four topics that will be covered as part of this agenda item:

Topic #1 – PKCS #12 Export Issue (initiated by NASA)

Topic #2 – Access to Protected Web Sites By People Outside the Hosting Agency's Enclave (Initiated by DoD and NASA)

Topic #3 – The Implementation Reality of PKI (initiated by DoD and NASA)

Topic #4 – Indicating Non-US Citizenship in Certificates (initiated by NASA)

Listed below are the discussion highlights and outcomes, in the order of discussion in the meeting.

Topic #2 & #3 --- The DoD PKI PMO has embarked on a mission to seek out any existing or develop their guidance about leveraging the benefits of cross-certification with the FBCA to improve business effectiveness for the full spectrum of DoD personnel. The DoD PKI PMO has established a Process Action Team (PAT) for this specific purpose and they have met once and will probably meet two more times to identify and collect requirements and issues related to PKI

interoperability and useful implementations. The FPKIPA is very interested in what DoD discovers in their requirements and issues identification and whatever guidance is found or generated. In parallel with this DoD study, the FPKIPA needs to consider if supplying general guidance and lessons learned about PKI implementations is part of its charter or if it should maintain its current focus of being a facilitator of establishing PKI interoperability via cross-certification process with the FBCA. DoD took an action to have this new PAT present a briefing to the FPKIPA at the 10 August FPKIPA meeting.

ACTION (078): DoD PAT will present a briefing at the 10 August FPKIPA meeting on the status of their PKI interoperability requirements and guidance research.

Topic #4 --- Various attendees contributed ideas of how to indicate citizenship in X.509 certificates, but none of the ideas solved the issue. Mr. Tim Polk volunteered to have NIST personnel work on this issue and report back to the FPKIPA at the 8 June meeting with a recommendation.

ACTION (079): NIST will develop a recommendation for how to indicate non-US citizenship in an X.509 certificate and present it at the 8 June FPKIPA meeting for consideration.

Topic #1 --- This topic was initiated because NASA is trying to decide if they are going to allow PKCS #12, even though it may introduce security problems. After some discussion, it was decided that this topic should be delegated to either the FPKI TWG or the FBCA TWG for technical resolution and the FPKI CPWG for policy resolution.

Agenda Item 6

Federal Identity Credentialing Committee (FICC) Report:

Ms. Judith Spencer reported that the Smart Card Policy and the Common PKI Policy (both available on the FICC website, <http://www.cio.gov/ficc>) have been approved by the FICC and forwarded to OMB. OMB accepted these policy documents without making any changes and is preparing the official memo to be part of the OMB clearing process to distribute them to all Federal agencies. This OMB memo also implements the FY2006 budget call and mandates that Federal organizations must use FICC policies if they are deploying Smart Cards or PKI for credentialing employees.

The Information Assurance Working Group held their last meeting on 6 May. They will need another meeting to approve the minimum requirements for Identity Proofing/Verification of Federal employees. These requirements are critical in the battle against identity theft, providing OMB guidance to agencies to make sure everyone does same minimum checks on new hires. DHS is very active in this working group.

Agenda Item 7

FPKI Certificate Policy Working Group (CPWG) Report:

Mr. Polk listed the following accomplishments since the March FPKIPA meeting:

- 1) Completion of 1st draft of FBCA CP reformat in the RFC 3647 format.

- 2) Mapping of Higher Education Bridge Certification Authority (HEBCA). This was a great mapping review because the HEBCA CP was a pretty straight-forward analysis and the technical interaction between the CPWG and HEBCA was mutually beneficial. Mr. Nathan Faut stated that Educause was very appreciative of the CPWG meeting and the technical/policy interaction. HEBCA will modify their CP, per the recommendations of the CPWG, before it is discussed again at a CPWG meeting and then a Mapping Report will be submitted to the FPKIPA to approve the HEBCA CP mapping.
- 3) The DoD ECA CP has been approved by the CPWG for mapping to the FBCA at the Medium level of assurance. The DoD ECA Mapping Report was distributed for review. There were no questions from the attendees. Here is the voting record:

Approval vote for the DoD ECA CP Mapping Report at the Medium level of assurance			
Voting members	Vote (Motion – Commerce; 2nd – Treasury)		
	Yes	No	Abstain
Dept of the Treasury	X		
Dept of Commerce	X		
Dept of Justice (proxy by FPKIPA Chair)	X		
Dept of Defense	CAN'T VOTE		
GSA	X		
OMB (proxy by FPKIPA Chair)	X		
NASA	X		
NFC (proxy by FPKIPA Chair)	X		

Ms. Spencer told the FPKIPA that she attended the US/Australian bilateral agreement meeting while she was in Australia in April. There was an agreement made as to how to manage the relationship between the Australian PKI (Gatekeeper) and the FBCA. The Australians will establish a CA in line with their CP and have subordinate CAs, rather than establish a Bridge CA, which was their original strategy.

Agenda Item 8

FBCA Operational Authority (OA) Report:

Status of FBCA Certification & Accreditation (C&A)

Mr. Darron Tate reviewed the status of the FBCA Certification & Accreditation, stating the following highlights:

- The FBCA OA is moving forward with plans and arrangements for a C&A with a full ATO, with a target completion date of 15 June 2004.
- ST&E was held on 22 April by KPMG. The main issue during ST&E was the emergency recovery process, but that was resolved the before the start of this FPKIPA meeting.
- Final review of C&A retest/findings will be done on 8 June 2004. The C&A approval letter should be signed on 15 June 2004.

The E-Governance Policy for Assurance Levels 1 & 2 (addressing server certificates) is needed. Compliance Audit of the FBCA must be done by the start of FY05 so this policy is needed fairly soon. CPWG already has the action (Action #075) to develop this E-

Governance Policy and it would be better to have it done by the end of July, to make sure it receives all the right approvals, rather than wait until closer to the start of FY2005. Ms. Cheryl Jenkins stated that she has written the Standard Operating Procedure (SOP) document for the FBCA OA to issue certificates using Level 1 and Level 2 authentication. Since this SOP is just for Level 1 and Level 2, the CPWG should review and give it an approval.

ACTION (080): FBCA OA will provide the Level 1 and Level 2 SOP to IATAC and IATAC will distribute to the CPWG for review and approval vote.

Status of FBCA/Applicant Cross-Certification Technical Testing:

A cross certificate was successfully issued to the Department of Energy on 27 April 2004.

Status of CA Testing:

Nothing new to report for CA Testing.

Agenda Item 9

Other Topics:

Action Item Review

No changes to the Action Item list were necessary at this time.

Agenda Item 10

Next Meeting Plans / Meeting Adjourned:

The next FPKI PA Meeting is scheduled for 8 June 2004 from 09:30-12:30 at the GSA facility located at 1800 F Street, Room 5141B, Washington, DC.

The meeting adjourned at 11:00 a.m.

D. LIST OF ATTENDEES

NAME	Email	Telephone	Organization
Alterman, Peter	altermap@mail.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
DeYoung, Tice	tdeyoung@hq.nasa.gov	202.358.2154	NASA
Dilley, Brian	brian.dilley@evalid8corp.com	443.250.7681	eValid8
Duncan, Steve	stephen.duncan@gsa.gov	202.708.7626	GSA
Faut, Nathan	nfaut@educause.edu	301.335.2656	HEBCA
Fenton-Menzies, Paul	paul.fenton-menzies@hic.gov.au	02.6124.6073	HIC (Australia)
Hanko, Dave	djhanko@missi.ncsc.mil	410.854.4900	DoD
Jenkins, Cheryl	cheryl.jenkins@gsa.gov	571.259.9923	GSA
Lentz, Mark	lentz_mark@bah.com	410.684.6520	IATAC
Marrie, Frederick	fmarrie@fdic.gov	703.516.1402	FDIC
Mitchell, Debbie	dmmittc3@missi.ncsc.mil	410.854.4900	DoD
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
Roche, Suzanne	suzanne.roche@hesa.com.au	02.6124.4268	HESA (Australia)
Tate, Darron	darron.tate@mitretek.org	703.610.1905	MTS

E. CURRENT ACTION ITEMS

No.	Action Statement	POC	Start Date	Target 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 Jan 2003</p> <p>Updated – 13 May 2003</p>	<p>13 Jan 2004</p> <p>FPKIPA meeting</p>	Open – reassigned to GSA/FTS, Cheryl Jenkins (as of 14 Jan 2003) and Tice DeYoung (13 May 2003)
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	13 Jan 2004 FPKIPA meeting	Open
048	Solicit participants with a real application to do business with Canada.	Judy Spencer, GSA	10 June 2003	13 Jan 2004 FPKIPA meeting	Open

No.	Action Statement	POC	Start Date	Target Date	Status
057	Write a short paper that says from here forward the FBCA OA will limit FBCA acceptance testing to systems that demonstrate enhanced assurance through NIAP testing.	Tim Polk, NIST	8 July 2003 Updated – 9 Sept 2003	9 Dec 2003 FPKIPA meeting	Open
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 Sept 2003	31 Dec 2003	Open
062	Define the NIAP certification requirement for future bridge membrane applications.	Tim Polk, NIST	9 Sept 2003	9 Dec 2003 FPKIPA meeting	Open
066	Develop text for the FPKIPA Charter regarding the sunset clause for voting members of the FPKIPA who are not cross certified members of the FBCA.	Tim Polk, NIST	18 Nov 2003	13 Jan 2003 FPKIPA meeting	Open
075	Develop, approve, and forward to the FPKIPA an E-Governance Certificate Policy for Assurance Levels 1 & 2 by 1 October 2004.	FBCA CPWG	9 Mar 2004	1 Oct 2004	Open
076	Check the accuracy of the dates and contact information in the Microsoft agreement (Action Item #68) and then distribute it to the FPKIPA and the CPWG.	FBCA OA	9 Mar 2004	13 Apr 2004 FPKIPA meeting	Open
078	Present a briefing at the 10 August FPKIPA meeting on the status of their PKI interoperability requirements and guidance research.	DoD PAT	11 May 2004	10 Aug 2004 FPKIPA meeting	Open
079	Develop a recommendation for how to indicate non-US citizenship in an X.509 certificate and present it at the 8 June FPKIPA meeting for consideration.	NIST	11 May 2004	8 June 2004 FPKIPA meeting	Open
080	Provide the Level 1 and Level 2 SOP to IATAC and IATAC will distribute to the CPWG for review and approval vote.	FBCA OA	11 May 2004	8 June 2004 FPKIPA meeting	Open