Federal Public Key Infrastructure Policy Authority (FPKIPA)
Minutes of the 8 August 2006 Meeting
GSA Headquarters Building, 18th and F Streets, NW, Washington, DC Room 7300

A.   AGENDA

1) Welcome & Opening Remarks / Introductions
2) Discussion / Vote on 11 July 2006 FPKIPA Minutes
3) SSP-WG Report
4) Review Policy Statement re Medium/Medium HW Certs on PIV Cards
5) FPKI Certificate Policy Working Group (CPWG) Report
   a) Update on the MIT Lincoln Laboratory LLC Mapping at Medium Hardware
   b) Update on the FBCA CP Omnibus Change Proposal: 2006-02
   c) Update on the Wells Fargo Non-IdenTrust Mapping (Basic and Medium Hardware)
6) FPKI Operational Authority (FPKI OA) Report
7) Final Meeting Items
   a) Legal Liability Issues of concern to Adobe
   b) NIST Memo regarding 800-53 CP-9
   c) SAFE Cross-Certification with the Federal Bridge
   d) NASA Weather Satellite
   e) Update on NIST FIPS 201 Memo re need to assert Common Policy OIDs by 2008
   f) September 12, 2006 FPKIPA Meeting
8) Adjourn Meeting

B.   ATTENDANCE LIST

VOTING MEMBERS

A quorum of ten (10) voting members present of fourteen (14) voting members, or 71%, where a quorum of 66.6% was required. GSA gave its proxy to HHS for this meeting. OMB continues to be an ex-officio member and the Department of Energy is currently a non-voting member because of its audit status.

NOTE: Contact information has been removed at the request of FPKIPA members. This information will be posted to a secure web site for FPKIPA members only at some point in the future. FPKIPA minutes already posted on the website will be redacted to remove POC information. FPKIPA members needing POC information on other members and participants should contact the Secretariat.

Organization	Name	Email	Telephone
Department of Commerce (NIST)	Dave Cooper		

Organization	Name	Email	Telephone
	(alternate for Tim Polk)		
Department of Defense	Mitchell, Deborah		Teleconference
Department of Energy	Not currently a voting member		
Department of Health & Human Services	Alterman, Peter		
Department of Homeland Security	Absent		
Department of Justice	Morrison, Scott		
Department of State	Absent		
Department of the Treasury	Absent		
Drug Enforcement Agency (DEA CSOS)	Jewell, Chris		
GPO	Hannan, John		
GSA (Proxy to HHS)	Temoshok, David by Proxy to HHS		
NASA	DeYoung, Tice		Teleconference
OMB	Ex-Officio Member		
USDA/NFC	Absent		
USPS	Stepongzi, Mark		
USPTO	Purcell, Art		

OBSERVERS

Organization	Name	Email	Telephone
Department of State (ManTech)	Froehlich, Charles R.		Teleconference
GSA	Duncan, Steve		Teleconference
DHS	Shomo, Larry		Teleconference
Legal Consultant	McDowell, Gene		
Enspier (Secretariat)	Fincher, Judy		
Wells Fargo	Drucker, Peri		Teleconference
FPKI/FICC support (FC Business Systems)	Petrick, Brant		

C.   MEETING ACTIVITY

Agenda Item 1

Welcome & Opening Remarks / Introductions—Dr. Peter Alterman
This meeting took place at the GSA Headquarters Building, 18th and F Streets, NW, Washington, DC, Room 7300. Dr. Peter Alterman of HHS and Chair of the FPKIPA called the meeting to order at 9:30 a.m. with attendee introductions. He complimented Rebecca Nielsen on her thorough review and revision of the

<u>Criteria and Methodology</u> (C&M) document, which she distributed to the C&M editing team last week.

Agenda Item 2

Discussion/Vote on 11 July 2006 FPKIPA Minutes—Ms. **Judy Fincher**

Ms. Fincher stated that she received substantive changes to the minutes and that a red-lined version had been distributed to the FPKIPA listserv prior to the August 8 FPKIPA meeting.

The vote on the minutes was postponed because a quorum did not exist when this item came up for a vote. The FPKIPA will vote on the 11 July minutes at the September 12, 2006 FPKIPA meeting. Ms. Fincher will distribute the red-lined version again prior to that meeting.

Agenda Item 3

SSP-WG Report— Steve Duncan

Steve Duncan stated that the scheduled August 16, 2006 SSP-WG meeting to review the submissions by Entrust and DST (IdenTrust) had been cancelled.

Dave Cooper had reviewed the submissions on behalf of the SSP-WG and found they needed additional work before they could be reviewed.

ACTION: On August 16, Steve Duncan and a sub-group of the SSP-WG will hold conference calls with Entrust and DST (IdenTrust) to provide insights into the changes they need to make to their CPS/matrices before the SSP-WG can review them again.

Agenda Item 4

Review Policy Statement re Medium/Medium HW Certs on PIV Cards— Judith Spencer

Judith Spencer distributed a draft Policy Statement to the FPKIPA listserv for comment prior to this meeting, but only Dr. Alterman responded.

In Judith Spencer's absence today, Dr. Alterman led the discussion. He defined the issue on the table: Do agencies have to upgrade to Medium Hardware by Oct. 27, 2006?

Most FPKI affiliates are cross-certified at Medium (software) which corresponds to E-Auth Level 3. Only Medium Hardware and High map to E-Auth Level 4 (required for HSPD-12), he said, adding that Basic maps to Level 3 and Rudimentary to Level 2.

To be compliant with HSPD-12 (FIPS 201), you have to issue Medium Hardware certs, Dr. Alterman said. Dave Cooper concurred.

This means that all FPKI Affiliates have to upgrade from Medium to Medium Hardware and that the FPKIPA has to cross-certify you at Medium Hardware. And, Dr. Alterman said, we need a strategy to get FPKI Affiliates upgraded and cross-certified at Medium Hardware before October 27, 2006. That's 80 days. Moreover, we need a way to fast-track these cross-certifications through the CPWG and FPKIPA.

Art Purcell (USPTO) made a motion to facilitate this process.

MOTION: Allow a process for fast tracking upgrades from Medium to Medium Hardware by having agencies submit only those changes identified in Judy Spencer's draft memorandum. The CPWG would only review these sections. If an agency has a policy that already satisfies Medium Hardware, it will provide a copy of its policy with pointers to those same sections. In all cases, the revised CPs will have to express the Medium Hardware OID.

This motion was seconded by GPO and was put to the vote. It passed with 10 votes (or a 2/3 majority of the 14 voting members). The voting record is shown on the next page.

ACTION: Dr. Peter Alterman is to send out a memo saying how we are going to upgrade agencies to Medium Hardware and in what timeframe. (Done)

ACTION: Dr. Alterman and Steve Duncan will talk about how the migration of FPKI agencies to Medium Hardware will affect the ACES agencies.

Approval vote for Motion to Upgrade Agencies to Medium Hardware			
Voting members	Vote (Motion – USPTO; 2nd – GPO)		
	Yes	No	Abstain
Department of Commerce	X		
Department of Defense	X		
Department of Energy	Not currently a Voting Member		
Department of Health & Human Services	X		
Department of Homeland Security	Absent-Did not Vote		
Department of Justice	X		
Department of State	Absent-Did not Vote		
Department of the Treasury	Absent-Did not Vote		
Drug Enforcement Agency (DEA CSOS)	X		
GPO	X		
GSA (Proxy to HHS)	X		
NASA	X		
OMB	Ex Officio Member		
USDA/NFC	Absent-Did not Vote		
USPS	X		
USPTO	X		

Agenda Item 5

FPKI Certificate Policy Working Group (CPWG) Report—Dave Cooper
a) Update on MIT Lincoln Laboratory LLC Mapping at Medium Hardware

Dave Cooper said that MIT had provided a response to the CPWG's second round of comments, but that we had not yet had time to review them.

ACTION: Dave Cooper will review the MIT response and make a recommendation as to whether or not they can be mapped at Medium Hardware to the CPWG at its August 15, 2006 meeting.

b) Update on the FBCA CP Omnibus Change Proposal: 2006-02

The CPWG reviewed the FBCA CP Omnibus Change Proposal: 2006-02 at its July 27 meeting. This version included the mapping impact assessment (performed by Enspier/Matt King). The CPWG at the 27 July meeting made several changes and instructed Mr. King to distribute the revised version, along with the mapping matrices, to the FPKIPA and CPWG listservs prior to the August 8 FPKIPA meeting.

This version also includes changes that fell out of discussions with the E-Auth PMO and with CertiPath, but does not yet include the OCSP requirements found in the Common Policy. It was agreed that the OCSP

requirements would be added to the FBCA CP when it is harmonized with the Common Policy—before the end of the year.

ACTION: Judy Fincher is to re-send the latest version of the FBCA CP Omnibus Change Proposal: 2006-02 to the FPKIPA listserv this week. This document will be voted on at the September 12, 2006 FPKIPA meeting. (Done)

c) Update on the Wells Fargo Non-IdenTrust Mapping (Basic and Medium Hardware)
Enspier has been tasked with performing the new mapping of the Wells Fargo Non-IdenTrust CP/CPS (Basic and Medium Hardware) and is doing the mapping this week.

During the mapping process, Mr. King will work in an iterative manner, identifying any tables that require revision--and corresponding sections of the Wells Fargo CP and/or Wells Fargo I&A document--and discussing them with Peri Drucker (Wells Fargo) at the earliest opportunity, so that she and her staff can make the necessary changes. This will allow Ms. Drucker to submit the revised CP/CPS and matrices to the CPWG in time for the August 15 meeting, where they will be reviewed again.

Ms. Drucker's concern was the timing of this effort. DoS and Treasury want to use our certs for their applications that are coming on board at the end of this month, she said.

Agenda Item 6

FPKI Operational Authority (FPKI OA) Report—Cheryl Jenkins

Ms. Jenkins was not present to give this report.

Agenda Item 7

Final Meeting Items—Dr. Peter Alterman
a) Legal Liability Issues of Concern to Adobe—John Hannan/GPO
John Hannan reported that John Landwehr of Adobe (and/or his legal representative) and John Cornell (GSA Attorney) had not yet held the conference call to discuss this issue.

ACTION: Judy Fincher is to remind Adobe that they requested a telephone conference between the GSA and Adobe lawyers to discuss legal liability issues of concern to Adobe. (Done)

b) NIST Memo regarding 800-53 CP-9

Dr. Alterman said that OMB in its memorandum OMB-8-16 had required encryption of everything that goes out. NIST then modified NIST SP 800-53 (Contingency Planning (CP-9) to require encryption whenever logs or records are taken off site.

The CPWG at its last meeting (audit workshop of August 3, 2006) discussed this new requirement and felt it was detrimental to the work of the FPKIPA. The CPWG requested Enspier to prepare a draft memo to NIST, requesting modification of Clause 4 of CP-9. Mr. King sent this draft memo to Dr. Alterman for review on 8/7/06 and he found it did not have a sufficiently compelling argument.

Dr. Alterman asked the FPKIPA members if we could satisfy the NIST encryption requirement (NIST SP 800-53, CP-9) without shutting down our ops.

ACTION: Matt King (Enspier) is to send the memo to the FPKIPA and CPWG/Audit WG for their review. Members are to provide the following information: 1. Rationale for why the FPKIPA should get involved and address this issue with NIST and, 2. Any compelling arguments that will be sufficient to convince NIST that there are valid reasons why they should not "raise the bar" in this particular area. (Done)

ACTION: Judy Fincher (Secretariat) is to ask Cheryl Jenkins to generate an email discussion topic on this issue. (Done)

Immediately after the meeting, Ms. Jenkins responded in an email that she saw this as an operational issue that she would work with Mitretek. Her approach will be to use the existing draft as the basis and incorporate any additional appropriate language. In her view, the compelling argument centers on operational expenses associated with encryption.

Art Purcell noted that his security expert at the USPTO (Greg McCain) estimated a 15% lag when you are encrypting data.

c) **SAFE Cross-Certification with the Federal Bridge**
On 8/7/06 Dr. Alterman and Judy Fincher (Secretariat) met with Jerry Zagar of Northrop Grumman, who is in charge of technical policy for SAFE, the pharmaceutical PKI bridge. As a result of that meeting, Dr. Alterman reported that SAFE will be cross-certifying with the Federal Bridge at Medium CBP and Medium Hardware CBP in the October 2006 timeframe. SAFE currently has 18 cross-certified members and two operational applications (HHS/National Cancer Institute and FDA).

At that meeting, we agreed both would follow Part III (Bridge-to-Bridge) of the Criteria and Methodology document.

ACTION: Dr. Alterman will issue a memo to SAFE, capturing the agreements of his 8/7/06 meeting with SAFE (Jerry Zagar).

d) **NASA Weather Satellite**

Tice DeYoung (NASA) reported on a joint project of DoD, Commerce and NASA (and their vendors/contractors)--the next generation weather satellite. This group of contractors (Northrop Grumman, Raytheon, etc) needs device certs to be used for the uplink and downlink from satellites and for ground station terminals.

The FPKIPA Chair and NASA agreed this might be a good application for CertiPath.

ACTION: Judy Fincher is to set up a conference call between CertiPath, Dr. Alterman and Dr. DeYoung this week to discuss using CertiPath certs (from either Northrop Grumman or Raytheon) for this purpose.

e) **Update on NIST FIPS 201 Memo re need to assert Common Policy OIDs by 2008**

Debbie Mitchell (DoD) asked for a status update on the memo from the FPKIPA Chair to NIST requesting that NIST revoke the FIPS 201-1 requirement that entities cross-certified with the Federal Bridge assert the Common Policy OIDs by January 1, 2008.

The comment period ended June 16, 2006 and Tim Polk had indicated we should receive some preliminary feedback by the end of June. At the last CPWG meeting (August 3, 2006), Mr. Polk stated that this request was presented to the Executive Steering Committee (ESC) at their last meeting.

Dave Cooper reported that Mr. Polk is concerned over this legacy PKI issue. What changes need to be made to the Common Policy if NIST does not agree with our request?

Ms. Mitchell stated that DoD could not come into compliance with the Common Policy unless the requirement is rescinded. DoD has stopped work on Common Policy comments until NIST resolves this issue, she said. If NIST does not act in our favor, will it be necessary to issue a new type of policy OID in 2006?

It was noted that both DoD and NASA are voting members of the ESC.

ACTION: Judy Fincher is to put this item [Update on NIST FIPS 201 Memo re need to assert Common Policy OIDs by 2008] on the CPWG agenda for the August 15 meeting. (Done)

f) September 12, 2006 FPKIPA Meeting
The September 12, 2006 FPKIPA meeting will be held at the Federal Trade Commission, 601 New Jersey Ave., NW, Washington, DC-Conference Room B. Directions will be sent along with the meeting announcement/agenda.

Agenda Item 8

Adjourn Meeting
The meeting adjourned at 11:00 a.m.

CURRENT ACTION ITEMS

No.	Action Statement	POC	Start Date	Target Date	Status
187	Mr. Tim Polk and Ms. Judy Spencer will meet with DoD to conceptualize a plan to help DoD internally to upgrade its CA's and shore up its infrastructure (repositories).	Judy Spencer, Debbie Mitchell	10 Jan. 2006	Sept. 2006	**Open**
189	We need to revise the MOA to accommodate E-Auth Federation requirements. Defer to after the E-auth PMO changes the Legal and Business Rules.	Peter Alterman, John Cornell, Georgia Marsh (or PMO rep)	20 July 2006	Oct.-Nov., 2006	**Open**
191	Mr. Art Purcell will be put on the work team to provide information on federal regulations that govern storage of the documents that will be posted to the shared Document Management Services system on behalf of the Policy Authority.	Cheryl Jenkins, Art Purcell	10 Jan. 2006	14 Feb. 2006	**Open**
193	Dr. Peter Alterman and the head of the OA will negotiate terms for the cross-certification process and add this language to the By-Laws document. This will be brought to the Policy Authority for a vote. (To coincide with Action Item # 189).	Dr. Peter Alterman, Cheryl Jenkins	10 Jan. 2006	Oct.-Nov. 2006	**Open**

No.	Action Statement	POC	Start Date	Target Date	Status
211	Ms. Judy Spencer is to speak with Acting Federal Acquisition Service Commissioner G. Martin Wagner regarding leasing other space at the Willow Woods facility for the FPKIA operations center.	Judy Spencer	14 March 2006	31 March 2006	Open
212	Ms. Cheryl Jenkins is to develop an Approach to Application Testing for PD-Val.	Cheryl Jenkins	14 March 2006	8 Aug. 2006	Open
221	Mr. Randy Speed is to inform the FPKIPA when the NFC no longer has any certificates, so that the NFC cross-certification can be revoked.	Randy Speed	9 May 2006	30 Sept. 2006	Open
228	Judith Spencer will draft a policy statement regarding Medium/Medium Hardware certs on PIV cards.	Judith Spencer	11 July 2006	8 August 2006	Open
229	Judith Spencer agreed to put together a proposal for review of the 3647 formatted CPs. This proposal should cover how agencies handle the timing of the upgrade, how to integrate with their CPS, and how to shortcut the process.	Judith Spencer	11 July 2006	8 August 2006	Open
230	Tim Polk of NIST, the Department of Commerce representative to the FPKIPA and member of the review committee, will push to have the FPKIPA's concerns addressed. He will notify the FPKIPA via email as to the decision of NIST regarding the memo, probably before the end of the month.	Tim Polk	11 July 2006	8 August 2006	Open
234	The SSP re-write committee headed by Dr. Peter Alterman will create a new section 4 of the Crits and Methods (C&M) document for SSPs. This will bleed into the FPKIPA Charter and By-Laws. Dr. Alterman said the C&M re-write will be analogous to what we did with ACES, i.e., we ask for their bona fides: memo of application, 800-79 compliance statement, and audit summary.	Peter Alterman, et al	11 July 2006	8 August 2006	Open
235	John Hannan will set up a meeting with John Landwehr (Adobe) and John Cornell (GSA) to discuss legal liability issues of concern to Adobe	John Hannan, John Landwehr, John Cornell	11 July 2006	8 August 2006	Open

No.	Action Statement	POC	Start Date	Target Date	Status
236	On August 16, Steve Duncan and a sub-group of the SSP-WG will hold conference calls with Entrust and DST (IdenTrust) to provide insights into the changes they need to make to their CPS/matrices before the SSP-WG can review them again.	Steve Duncan	8 August 2006	11 August 2006	Open
237	Dr. Alterman and Steve Duncan will talk about how the migration of FPKI agencies to Medium Hardware will affect the ACES agencies.	Peter Alterman, Steve Duncan	8 August 2006	12 Sept. 2006	Open
238	Dave Cooper will review the MIT response and make a recommendation as to whether or not they can be mapped at Medium Hardware to the CPWG at its August 15, 2006 meeting.	Dave Cooper	8 August 2006	15 August 2006	Open
239	Dr. Alterman will issue a memo to SAFE, capturing the agreements of his 8/7/06 meeting with SAFE (Jerry Zagar).	Peter Alterman	8 August 2006	11 August 2006	Open
240	Judy Fincher is to set up a conference call between CertiPath, Dr. Alterman and Dr. DeYoung this week to discuss using CertiPath certs (from either Northrop Grumman or Raytheon) for this purpose.	Judy Fincher	8 August 2006	11 August 2006	Open