Federal Public Key Infrastructure Policy Authority (FPKIPA)

Minutes of the 13 November 2007 Meeting

USPS Headquarters, 475 L'Enfant Plaza, SW, Washington, DC
Conference Room: 2P316 (inside room 2P310)

A. AGENDA

1. Welcome / Introductions
2. Discussion / Vote on 11 September 2007 FPKIPA Minutes
3. Discussion / Vote on 9 October 2007 FPKIPA Minutes
4. FPKI Certificate Policy Working Group (CPWG) Report
    1) *Discuss / Vote on Revised C4CP – Dave Cooper*
    2) *University of Texas Update – Matt King*
    3) *Wells Fargo Medium and Medium Hardware Revised CP Discussion/Report – Judith Spencer, Dr. Peter Alterman*
    4) *Discuss / Vote Common Policy CP Change Proposal: 2007-03 – Judith Spencer, Dave Cooper*
    5) *Use of FAQs for FPKIPA – Dave Cooper, Dr. Peter Alterman*
5. Discuss DoD Algorithm Transition Plan – Sam Schaen (DISA, contractor, MITRE)
6. FPKI Operational Authority (FPKI OA) Report – Cheryl Jenkins
    1) *Certificate Directory Status – Wendy Brown*
    2) *Status of Common Policy Key Rollover – Wendy Brown*
    3) *SAFE Interoperability Testing – Cheryl Jenkins*
    4) *Test Environment Presentation – Terry McBride*
7. *Discuss / Vote to Cross-Certify MIT Lincoln Laboratory at Medium and Medium Hardware*
8. *Update on* SSPWG Activities
    1) 11 October 2007 SSP Vendor Meeting – Judith Spencer
9. Final Meeting Items
10. Adjourn Meeting

B. ATTENDANCE LIST

VOTING MEMBERS

The meeting began with a quorum of 12/15 (or 80%), where a two-thirds majority was required. One member joined the meeting after the quorum was established.

We redacted contact information in the published FPKIPA minutes 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 have been redacted to remove POC information. FPKIPA members needing POC information on other members and participants should contact the Secretariat at Judith.fincher@enspier.com.

Organization	Name	Telephone
Department of Commerce (NIST)	Cooper, David	
Department of Defense	O'Brien, Shawn	Teleconference
Department of Health & Human Services	Alterman, Dr. Peter	
Department of Homeland Security	Proxy to HHS/joined by Don Hagerling	
Department of Justice	Morrison, Scott	
Department of State	McCloy, Mark A.	
Department of the Treasury	Schminky, Jim	Teleconference

Organization	Name	Telephone
Drug Enforcement Administration (DEA CSOS)	ABSENT	
GPO	Hannan, John	
GSA / ALTERNATE	Spencer, Judith, joined by David Temoshok	
NASA	DeYoung, Tice	Teleconference
Nuclear Regulatory Commission- NRC	Sulser, David	
SSA	Proxy to HHS	
USPS	Stepongzi, Mark	
USPTO	ABSENT	

OBSERVERS

Organization	Name	Telephone
FPKI/FICC Support (Contractor--General Dynamics Information Technology)	Petrick, Brant	
FPKIPA Secretariat (Contractor -- Enspier Technologies/Protiviti Government Services)	Fincher, Judy, Ph.D.	
DoD PKI PMO/DISA (Contractor, MITRE)	Schaen, Sam	
IdenTrust	Young, Kenny	
FPKI OA (Contractor—Enspier Technologies/Protiviti Government Services, Technical Lead)	Brown, Wendy	
FPKI OA (Contractor—Enspier Technologies/Protiviti Government Services, Lab Manager)	McBride, Terry	
FPKI OA/GSA (PM)	Jenkins, Cheryl	
Wells Fargo	Drucker, Peri	Teleconference
NRC (Contractor, VeriSign)	Evans, Frazier	
KPMG	Nazario, Noel	
eValid8 (Contractor)	Dilley, Brian	
FPKI/FICC/GSA	Spencer, Judith	
Enspier/Protiviti Government Services	King, Matt	Teleconference
Department of State/Senior Policy Analyst (Contractor, ManTech)	Froehlich, Charles	

C. MEETING ACTIVITY

Agenda Item 1

Welcome / Introductions—Dr. Peter Alterman, Chair

The FPKIPA met at the USPS Headquarters Building, 475 L'Enfant Plaza, SW, Washington, DC, Conference Room: 2P316 (inside room 2P310). Dr. Peter Alterman, Chair, called the meeting to order at 9:43 a.m. with the attendee roll call. We wish to thank Mr. Mark Stepongzi of the USPS for hosting this meeting.

Agenda Item 2

Discussion / Vote on 11 September 2007 FPKIPA Minutes—Judy Fincher

Ms. Fincher said that she had incorporated all the comments received and distributed a redline version of the revised 11 September 2007 minutes to the FPKIPA five working days prior to the 13 November 2007 FPKIPA meeting. The FPKIPA voted by 73% (11/15) to approve the minutes, as amended, where a 50% majority vote was required. Three members were absent and one member abstained.

NOTE: The FPKIPA voted without a motion and second having been made.

Approval vote for 11 September 2007 FPKIPA Minutes			
Voting members	**Vote (Motion – ; 2nd –)**		
	Yes	**No**	**Abstain**
Department of Commerce			√
Department of Defense	√		
Department of Health & Human	√		
Department of Homeland Security - Proxy to HHS	√		
Department of Justice	√		
Department of State	√		
Department of the Treasury	√		
Drug Enforcement Administration (DEA CSOS)	ABSENT		
GPO	√		
GSA	√		
NASA	ABSENT FOR THIS VOTE		
Nuclear Regulatory Commission (NRC)	√		
SSA - Proxy to HHS	√		
USPS	√		
USPTO	ABSENT		

Agenda Item 3

Discussion / Vote on 9 October 2007 FPKIPA Minutes—Judy Fincher

Ms. Fincher said she incorporated all the comments received and distributed a redline version of the revised 9 October 2007 minutes five working days prior to the 13 November 2007 FPKIPA meeting. The FPKIPA voted by 66.7% (10/15) to approve the minutes, as amended during the 13 November 2007 meeting and in the redline document, where a 50% majority vote was required. Two members abstained and three members were absent.

NOTE: The FPKIPA voted without a motion and second having been made.

Approval vote for 9 October 2007 FPKIPA Minutes			
Voting members	**Vote (Motion – ; 2nd –)**		
	Yes	**No**	**Abstain**
Department of Commerce			√
Department of Defense	√		
Department of Health & Human Services	√		
Department of Homeland Security - Proxy to HHS	√		
Department of Justice	√		

Department of State			√
Department of the Treasury	√		
Drug Enforcement Administration (DEA CSOS)	ABSENT		
GPO	√		
GSA	√		
NASA	ABSENT FOR THIS VOTE		
Nuclear Regulatory Commission (NRC)	√		
SSA- Proxy to HHS	√		
USPS	√		
USPTO	ABSENT		

Agenda Item 4

FPKI Certificate Policy Working Group (CPWG) Report—Dave Cooper, et al.

1) *Discuss/Vote on the Revised C4CP*

There was heated discussion on this topic. Peri Drucker pointed out that entities at C4 could not say they were cross-certified with the Federal Bridge, because they are not. She wanted to know how the OIDs are expressed.

Dr. Alterman said the C4 Policy is for non-Federal "sub-basement" PKIs who cannot aspire to strong authentication, such as the GRID PKIs and VeriSign Open PKI Class 2.

Judith Spencer said the FPKIPA needs this policy for those entities who cannot meet Federal Bridge cross-certification requirements, but who need an E-Authentication Level 2 credential.

The FPKIPA failed to approve the revised C4CP. A 75% majority vote was required; and the "Yes" vote was 11/15, or 73%.

Vote to Approve Revised C4CP			
Voting members	**Vote (Motion – GSA ; 2nd – State)**		
	Yes	**No**	**Abstain**
Department of Commerce		√	
Department of Defense	√		
Department of Health & Human Services	√		
Department of Homeland Security– Proxy to HHS	√		
Department of Justice	√		
Department of State	√		
Department of the Treasury	√		
Drug Enforcement Administration (DEA CSOS)	ABSENT		
GPO	√		
GSA	√		
NASA			√
Nuclear Regulatory Commission (NRC)	√		
SSA– Proxy to HHS	√		

USPS	√		
USPTO	ABSENT		

ACTION: Judith Spencer said we should post an explanation of the purpose of the C4CP to the FPKIPA website, explaining that the FPKIPA needs this policy for those entities who cannot meet Federal Bridge cross-certification requirements, but who need an E-Authentication Level 2 credential.

ACTION: Judy Fincher (Secretariat) will conduct an e-vote on C4CP the week of November 26, 2007.

2) *University of Texas Update – Matt King*
Matt King said the University of Texas requirement is to map at C4 next month. Although the old C4 policy is still in effect, because of the above vote, UT will be mapping against the new C4CP, he said.

3) *Wells Fargo Medium and Medium Hardware Revised CP Discussion/Report – Judith Spencer, Dr. Peter Alterman*
Judith Spencer reported on her recent trip to San Francisco to meet with Wells Fargo (Peri Drucker and Jim Gross), along with Dr. Peter Alterman and Matt King. The FPKI team went through the list of 12 discussion items identified by the CPWG, explaining the issues and getting Wells Fargo's comments. This process was somewhat hampered by the fact that Wells Fargo had only recently submitted (the week before) a revised CP which purported to respond to the CPWG's 12 issues; they also submitted an errata list 24 hours before the meeting began. The CPWG will review the Wells Fargo response.

A side benefit of the trip was a presentation from Wells Fargo under a Non-Disclosure Agreement (NDA) on the Wells Fargo architecture and business processes. This background information will inform the discussion of the Wells Fargo operational issues by the CPWG at a subsequent meeting.

Dr. Alterman said that he and Judith Spencer also visited with the head of the Liberty Alliance and that more information would be provided at a later meeting.

4) *Discuss / Vote Common Policy CP Change Proposal: 2007-03 – Judith Spencer, Dave Cooper*
This Change Proposal, drafted by Judith Spencer and Dave Cooper, is intended to allow legacy PKI's to comply with FIPS 201. The changes allow legacy PKI's to employ the PIVAuth credential. This will be a brand-new certificate for all legacy PKI's that are Medium Hardware or higher, Ms. Spencer said.

David Cooper raised an operational issue that derailed the attempt to move to a vote at this meeting. He wanted to know: if a legacy PKI was cross-certified at Medium Hardware, can we assume they are compliant with PIVAuth? Can they use the Common Policy OIDs?

Ms. Spencer said, "Yes," and noted we have no other way of signifying it. And, she said, these differences do not affect the mapping.

Dave Cooper said that there are two issues: policy and conformance. How do we determine conformance?

Charles Froehlich asked if their CP and/or CPS would have to assert the appropriate Common Policy OIDs, or would that be assumed?

Dave Cooper: Can you have two governing documents, e.g., CPs?

Brian Dilley pointed out that from a compliance audit point of view, the CP and CPS must agree, therefore it would appear that both documents would have to include the appropriate OIDs.

ACTION: The FPKIPA sent Common Policy CP Change Proposal: 2007-03 back to committee where the remaining issues are to be re-worked by Judith Spencer and Dave Cooper. The FPKIPA may have the opportunity to vote on this proposed change at the 11 December 2007 FPKIPA meeting.

There was a side discussion about DoD being designated a "transitional agency" by OMB regarding the use of PIV cards. They were given a "bye" from OMB because they are a legacy smart card issuing agency with a large installed base of non-complaint CAC cards, i.e., they are not 2048-bit compliant.

5) *Use of FAQs for FPKIPA – Dave Cooper, Dr. Peter Alterman*
Dr. Alterman said that the FPKIPA will stand-up a web page with FAQs to answer questions frequently posed to the FPKIPA and its technical committees, such as, 1) requirements associated with key management keys in hardware, 2) cert suspension.

The FPKIPA agreed with John Hannan's suggestion that FAQ content be approved by the FPKIPA before it is posted on the web site because only the FPKIPA can make and/or interpret policy. In addition, the FPKIPA agreed to use e-votes as the routine method for approving FAQ text. Dr. Alterman said the By-Laws should be amended to reflect this change in procedure.

Agenda Item No. 5

Discuss DoD Algorithm Transition Plan—Sam Schaen (DISA/MITRE)

Sam Schaen, a MITRE contractor with DISA, made a presentation explaining DoD's Algorithm Transition Plan, which includes possible use of elliptical curve (ECC Suite B) technology. Dr. Alterman said that interoperability with ECC Suite B may be an issue, but that the FPKIPA will address that later.

The upshot of Mr. Schaen's presentation was that DoD is asking for a three to six-month reprieve to move their signing certs to 2048-bit technology. DoD proposes to start signing most new cards with 2048-bit keys in March 2008; by June 2008, all CAC cards would be signed by 2048-bit keys. The FPKIPA has a no-waiver policy.

ACTION: Dr. Alterman asked that the DoD submit the previously promised issues paper describing 1) the issues, 2) decisions, 3) commitments to distribute in November, for discussion at the 11 December 2007 FPKIPA meeting.

ACTION: An ad hoc working group comprised of Dr. Tice DeYoung, Jim Schminky, Judith Spencer, Dr. Peter Alterman, the "right" NIST person, and a representative from the Department of State (Charles Froehlich?) is empowered to review the DoD Issues Paper and make a recommendation to the FPKIPA.

David Temoshok said the Policy Authority may have to address making exceptions to FPKIPA and NIST SP 800-78-1 policies. Since DoD is a transitional agency (as per OMB), how much of the requirement does DoD have to follow? He said that OMB likely will adopt whatever the FPKIPA and NIST recommend.

Charles Froehlich noted that DoD (as per CTO 02-06) requires DoD certs to get into the numerous applications that DoD operates for the Federal Government, such as requests for symmetric key. Other agencies cannot get into the DoD applications now, and once other agencies have gone to SHA-256/RSA-2048, and/or DoD moves to ECC, it will be even more difficult.

Agenda Item No. 6

FPKI Operational Authority (FPKI OA) Report— Cheryl Jenkins, Wendy Brown

1. *Certificate Directory Status*
    a. Ms. Brown said the OA had issued two certs and revoked one.
    b. Dr. Tice DeYoung reported that NASA's migration is 65% complete and that their drop dead date is December 1, 2007. He will let Ms. Brown know when to revoke the old NASA cert.

2. *Status of Common Policy Key Rollover – Wendy Brown*
   Ms. Brown said that the new certificate issuance for Entrust, CertiPath and two of ORC's three were completed. ORC's third certificate request from their ACES Gov Certificate Authority is on hold until hardware issues are resolved. Ms. Brown went on to say that the OA has not yet received certificate requests from Treasury for either of their SSPs customers, so none has been issued. Exostar is not yet ready to make a certificate request, and VeriSign is waiting for their policy to be mapped at Medium-Hardware to exchange new cross-certificates. Otherwise, VeriSign and the OA will move forward with the posting of the cross-certificate pairs at Medium assurance level.

3. *SAFE Interoperability Testing – Cheryl Jenkins*
   Terry McBride said the SAFE interoperability testing would start on 14 November 2007.

4. *Test Environment Presentation -- Terry McBride*
   Mr. McBride said the FPKIA TWG had recommended and approved requirements and a Service Level Agreement (SLA) for a test environment on August 25, 2006. Since then, the requirements and SLA were drafted and a cost analysis was developed and

presented. He pointed out that the NIST test suites do not adequately mirror the FPKIA production environment. The FPKIA is far more complex than the NIST test suites, he said.

During the mirrored presentation slide, Brian Dilley wanted to know where the physical instance of the test environment is. Mr. McBride said it was sufficient to have a logical mirror instance of the affiliate's information—which does not include all physical components of entities' physical instances.

Mr. McBride said it is not the responsibility of the FPKI OA to troubleshoot validation products that have not been certified.

Several people questioned the need for 99.5% uptime for test environments. Ms. Jenkins said that the rationale is that everybody will be able to test at anytime. While the test environment has high availability, technical support does not have to be 24x7. It is sufficient to respond to test incidents during normal working hours, if necessary.

Mr. McBride presented information on costing scenarios for 1) entities with no existing test environment; 2) entities with an ad hoc test environment; and 3) entities with a mature test environment.

ACTION: Dr. Alterman will develop and distribute a questionnaire for the FPKIPA cross-certified members as a follow-up to the test environments requirements.

Agenda Item No. 7

Discuss / Vote to Cross-Certify MIT Lincoln Laboratory at Medium and Medium Hardware
The FPKIPA approved the MIT Lincoln Laboratory Cross-Certification at Medium and Medium Hardware on July 10, 2007, so the vote taken during the 13 November 2007 FPKIPA meeting (86.7% in favor) was unnecessary and duplicative. The measure passed with 100% on July 10, 2007. (See July 10, 2007 FPKIPA Minutes on the FPKIPA web site: http://www.cio.gov/fpkipa/documents/minutes_071007.pdf)

Dr. Alterman said he is in negotiations with MIT Lincoln Laboratory on the MOA. He will issue the LOA once the MOA is completed.

Agenda Item No. 8

Update on SSPWG Activities—Judith Spencer

11 October 2007 SSP Vendor Meeting

Ms. Spencer said she held a meeting on October 11, 2007 with the SSP vendors to discuss the C&A process. She has commissioned a study of the methodologies used by the SSPs for C&As and will compare these methodologies to NIST 800-53-A and NIST SP 800-37. Richard Wilsher, an independent third party expert, is conducting this review.

Ms. Spencer also said that GSA does the C&A on the core systems of SSPs. Entrust is the vendor supporting the MSO. As such, the GSA IG is auditing the C&A of Entrust this year.

Agenda Item 9

Final Meeting Items

a) The next FPKIPA meeting is a combination meeting/holiday party. Please bring holiday eats to share. The meeting is scheduled for 11 December 2007 (9:30 a.m. – noon at the GSA National Capital Region Building at 7th and D Streets, SW, Washington, DC, in room 5700 (accessed via Room 5060)

b) ACTION: David Temoshok requested that the Secretariat update the FPKIPA Monthly Status Sheet for each FPKIPA meeting (e.g., on a monthly basis).

c) Judith Spencer announced that the FPKI OA is now under the Office of Governmentwide Policy at GSA.

Agenda Item 10

Adjourn Meeting

The meeting adjourned at 11:47 a.m.

CURRENT ACTION ITEMS

No.	Action Statement	POC	Start Date	Target Date	Status
285	Judith Spencer and DoD will go off-line to discuss name uniqueness. She suspects there is name collision.	Judith Spencer, Debbie Mitchell	8 May 2007	22 May 2007	Open
303	The FPKIPA asked that Tim Polk prepare a written rationale for these changes, since the weakness of SHA-1 and 1024 bit keys is of great concern to many members and extending their lifetime may increase the threat that these algorithms be compromised	Tim Polk	10 July 2007	14 August 2007	Open
311	Debbie Mitchell volunteered to draft a memo for OMB signature that Mary Dixon will present at the next ESC.	Debbie Mitchell	14 Aug. 2007	11 Sept. 2007	Open
315	Cheryl Jenkins will generate the SAFE Interoperability Test Report once it is determined that all remaining issues have been resolved.	Cheryl Jenkins	9 Oct. 2007	19 Oct. 2007	Open

No.	Action Statement	POC	Start Date	Target Date	Status
315	Dr. Alterman and John Cornell will incorporate language into the FPKIPA audit Cook Book." This language was provided by Noel Nazario of KPMG and says that if customers set up the terms of their Web Trust audits appropriately, the Web Trust audit would satisfy all our requirements.	Dr. Alterman, John Cornell	9 Oct. 2007	13 Nov. 2007	Open
316	Judith Spencer said we should post an explanation of the purpose of the C4CP to the FPKIPA website, explaining that the FPKIPA needs this policy for those entities who cannot meet Federal Bridge cross-certification requirements, but who need an E-Authentication Level 2 credential.	??	13 Nov. 2007	26 Nov. 2007	Open
317	Judy Fincher (Secretariat) will conduct an e-vote on C4CP the week of November 26, 2007.	Judy Fincher	13 Nov. 2007	26 Nov. 2007	Open
318	The FPKIPA sent Common Policy CP Change Proposal: 2007-03 back to committee where the remaining issues are to be re-worked by Judith Spencer and Dave Cooper. The FPKIPA may have the opportunity to vote on this proposed change at the 11 December 2007 FPKIPA meeting	Judith Spencer, Dave Cooper	13 Nov. 2007	27 Nov. 2007	Open
319	Dr. Alterman asked that DoD prepare an issues paper describing 1) the issues, 2) decisions, 3) commitments to distribute in November, for discussion at the 11 December 2007 FPKIPA meeting.	Debbie Mitchell	13 Nov. 2007	4 Dec. 2007	Open
320	An ad hoc working group comprised of Dr.Tice DeYoung, Jim Schminky, Judith Spencer, Dr. Peter Alterman, the "right" NIST person, and a representative from the Department of State (Charles Froehlich?) is empowered to review the DoD Issues Paper and make a recommendation to the FPKIPA.	Dr. Alterman, et al.	13 Nov. 2007	3 Dec. 2007	Open
321	Dr. Alterman will develop and distribute a questionnaire for the FPKIPA cross-certified members about the status of their test environments.	Dr. Alterman	13 Nov. 2007	20 Nov. 2007	Open