Federal Public Key Infrastructure Policy Authority (FPKIPA)

DRAFT Minutes of the 9 October 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. Results of the two e-votes
    1) FBCA CP Change Proposal: 2007-05 (NIST SP 800-78-1)
    2) Common Policy CP Change Proposal: 2007-02 (DN)
4. FPKI Certificate Policy Working Group (CPWG) Report
    1) *Discuss / Vote on Revised C4CP*
    2) *Review the CPWG Recommendation re Accepting the MIT Lincoln Laboratory Audit Letter*
    3) *Review the CPWG Recommendation re Accepting the SAFE Bridge Mapping at Medium CBP and Medium Hardware CBP*
    4) *Wells Fargo Mapping at Medium CBP and Medium Hardware CBP*
    5) *Key Recovery Policy for the Common Policy SSPs*
5. FPKI Operational Authority (FPKI OA) Report
    1) *Certificate Directory Status*
        a. *Certificates Issued*
        b. *Certificates Revoked*
        c. *Certificates Fixed*
    2) *Issues in Progress*
    3) *Common Policy Key Rollover Status*
6. SSPWG Ad hoc Report
    1) First Responder and other "Comparability" Initiatives
    2) SSP C&A Guidance
    3) What it Means to be HSPD-12 "Compliant"
    4) October 11 2007 SSP Vendor Meeting
7. Adjourn Meeting

B. ATTENDANCE LIST

VOTING MEMBERS

The meeting began without a quorum, but reached a quorum of 11 voting members of 15 (73%) after Agenda Item # 4, where a two-thirds majority was required.

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)	ABSENT	
Department of Defense	Mitchell, Deborah	Teleconference
Department of Health & Human Services	Alterman, Dr. Peter	
Department of Homeland Security	ABSENT	
Department of Justice	Morrison, Scott	
Department of State	Proxy to HHS	

Organization	Name	Telephone
Department of the Treasury	Schminky, Jim	
Drug Enforcement Administration (DEA CSOS)	Jewell, Chris	Teleconference
GPO	Hannan, John	
GSA / ALTERNATE	Spencer, Judy	
NASA	DeYoung, Tice	Teleconference
Nuclear Regulatory Commission (NRC)	Sulser, David	
SSA	ABSENT	
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.	
DHS (Contractor, Cygnacom)	Shomo, Larry	Teleconference
SSA (Contractor, Jacob & Sundstrom)	Simonetti, David	Teleconference
IdenTrust	Corbo, Page	
IdenTrust	Young, Kenny	
FPKI OA (Contractor—Enspier Technologies/Protiviti Government Services, Technical Lead)	Brown, Wendy	
State of Illinois	Anderson, Mark	Teleconference
State of Illinois (PMA Chair)	Falzone, Val	Teleconference
FPKI OA/GSA (PM)	Jenkins, Cheryl	Teleconference
Wells Fargo	Drucker, Peri	Teleconference
NRC (Contractor, VeriSign)	Evans, Frazier	Teleconference
KPMG	Faut, Nathan	
eValid8	Dilley, Brian	
SSA	Kessler, Greg	Teleconference

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 9:40 a.m. with the attendee roll call. We wish to thank Mr. Mark Stepongzi of the USPS for hosting the meeting.

Agenda Item 2

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

Ms. Fincher said that she had not had the opportunity to incorporate comments received today from the DoD. Therefore, the FPKIPA will vote on the 11 September 2007 minutes at the 13 November 2007 meeting.

Agenda Item 3

Results of the two e-votes—Judy Fincher

Ms. Fincher presented the results of the two e-votes conducted last month:

1) FBCA CP Change Proposal: 2007-05 (NIST SP 800-78-1)
   Ms. Fincher said that this e-vote passed by 13/15, or 86.7% where a ¾ majority vote was required. There were two "No" votes. See the voting results, below:

Results of e-vote on FBCA CP Change Proposal: 2007-05 (NIST SP 800-71-1)			
Voting members	**Vote (Motion – N/A ; 2nd –N/A)**		
	Yes	**No**	**Abstain**
Department of Commerce	√		
Department of Defense		√	
Department of Health & Human Services	√		
Department of Homeland Security	√		
Department of Justice	√		
Department of State	√		
Department of the Treasury	√		
Drug Enforcement Administration (DEA CSOS)	√		
GPO	√		
GSA	√		
NASA		√	
Nuclear Regulatory Commission (NRC)	√		
SSA	√		
USPS	√		
USPTO	√		

2) Common Policy Change Proposal: 2007-02 (DN)

Ms Fincher said the e-vote on this Change Proposal was nearly unanimous. Fourteen of the 15 voting members (or 93.3%) voted to approve this measure, where a ¾ majority vote was required. One member did not vote. See the voting results, below:

Results of e-vote on Common Policy CP Change Proposal: 2007-02 (DN)			
Voting members	**Vote (Motion – N/A ; 2nd –N/A)**		
	Yes	**No**	**Abstain**
Department of Commerce	√		
Department of Defense	√		
Department of Health & Human Services	√		
Department of Homeland Security	√		
Department of Justice	v		
Department of State	√		

Department of the Treasury	√		
Drug Enforcement Administration (DEA CSOS)	√		
GPO	√		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC)	DID NOT VOTE		
SSA	√		
USPS	√		
USPTO	√		

Agenda Item 4

FPKI Certificate Policy Working Group (CPWG) Report—Dr. Pete Alterman

In the absence of the Commerce representative and his alternate, Dr. Alterman made the CPWG report.

1) *Discuss/Vote on the Revised C4CP*

Dr. Alterman said we would vote on the C4CP at the13 November 2007 FPKIPA Meeting, to give members time to review the document.

2) *Review the CPWG Recommendation re Accepting the MIT Lincoln Laboratory Audit Letter*

Dr. Alterman said that the Secretariat distributed this recommendation prior to the meeting and that there were no issues.

3) *Review the CPWG Recommendation re Accepting the SAFE Bridge Mapping at Medium CBP and Medium Hardware CBP*

Dr. Alterman said that the Secretariat distributed this recommendation prior to the meeting and that there were no issues with the mapping. He said the FPKIPA would vote on the cross-certification with the SAFE Bio-pharmaceutical Bridge if all interoperability testing issues were resolved to our mutual satisfaction.

ACTION: Judy Fincher will contact Phil Welsh, the SAFE Technical POC, to see if any issues had arisen in SAFE's "reverse mode" testing.

ACTION: Cheryl Jenkins will generate the SAFE Interoperability Test Report once it is determined that all remaining issues have been resolved.

4) *Wells Fargo Mapping at Medium CBP and Medium Hardware CBP*
Dr. Alterman and Judith Spencer will meet with Wells Fargo's technical and policy team in San Francisco in early November to help Wells Fargo finalize their policies so that the CPWG can successfully map them to the FBCA CP.

5) *Key Recovery Policy for the Common Policy*
Dr. Alterman said that he, Judith Spencer and Dave Cooper are drafting a Key Recovery Policy for the Common Policy. This will be mapped as a Practice Statement and will be an auditable event.

Agenda Item No. 5

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

1) *Certificate Directory Status*
Ms. Brown said that there had been no directory outages since September 11 2007

a. Certificates Issued

- Ms. Brown said that the LOA and MOA for the DoD Interoperability Root are not in agreement. Dr. Alterman said the CPWG would review this issue at the October 16 2007 CPWG meeting.

- Ms. Brown said the OA expects to issue the Treasury Medium Hardware certificate with the FBCA this week. (by 10/12/07)

- The FPKI OA issued the USPS cross-certificate on 9/26/07, she said.

b. Certificates Revoked –None.

- Dr. Tice DeYoung asked the FPKI OA to wait until NASA migrates the remaining users to their new CA (by the end of October) and shut down the old CA before revoking the old cross-certificate. Dr. DeYoung will issue a request to revoke to the FPKI OA when the time is right. Dr. DeYoung said NASA had already migrated 13,609 users.

- DEA CSOS has changed contractors and will be shutting down their old CA and standing up a new one. Chris Jewell said he expects this to happen by the end of the month. Once the DEA CSOS notifies the FPKI Policy Authority that the cutover has occurred, Dr. Alterman will issue a request to the FPKI OA to revoke their CA certificate.

c. Certificates Fixed
The expired cross-certificate for the State of Illinois has been fixed. A new cross certificate pair has been posted in the Directory.

1) *Issues in progress*

a. DHS – The FPKI OA is waiting for a response on their directory issues.

ACTION: Dr. Alterman and Larry Shomo (DHS Contractor, Cygnacom) will talk offline next week to discuss the DHS plans for their PKI.

2) *Common Policy Key Rollover Status*

Ms. Brown explained that the technical approach to the Common Policy Key Rollover had changed. The FPKI OA is not standing up a new CA; they are doing a Rollover of the Microsoft CA. This is a re-key, she said. The FPKI OA's approach is now to perform a key rollover on the existing Microsoft CA. However, they have encountered problems with the Microsoft CA software and are working closely with Microsoft to resolve the remaining issues.

- One technical issue is that the Microsoft CA issues segmented CRLs. It does not automatically create a complete CRL containing all certificates revoked by both the old and new keys. Therefore, the FPKI OA will be adding a process to create and post a complete CRL for both the old and new keys.

- Another Microsoft limitation is the difficulty entailed in getting new policy OIDs included in the rollover certificates.

Ms. Jenkins said the FPKI OA is making progress in the laboratory and is making sure that SSPs have new certificates with a new validity period in the certificate. SSPs will be limited to issuing six-year certificates with new Policy OIDs.

Due to delays caused by Microsoft software issues, the FPKI OA now anticipates performing the rollover by Friday, October 12, 2007.

Judith Spencer wanted to know if the date slippage of the rollover will create problems for any of the SSPs. Ms. Jenkins said the only SSP vendor (Cybertrust) that had responded indicated there is a problem with the delay.

NOTE: This change in approach means that the name of the Common Policy Root CA will not change. The FPKIPA voted at the 11 September 2007 FPKIPA meeting to approve the name change, but this will no longer be necessary.

As an aside, Dr. Alterman said that Microsoft announced today that they are shipping Service Pack 3 for XP, which includes support for SHA-256.

Agenda Item No. 6

SSPWG Ad hoc Report—Judith Spencer

a. ***First Responder and other "Comparable" Initiatives***

Ms. Spencer said things are moving faster than anticipated in the greater identity management community. FIPS 201 has become the new "gold standard" for smart ID cards, she said. The commercial community wants the cards they are issuing to be recognized by Federal agencies and for the cards to interoperate with Federal agencies.

DHS is leading the charge for the "first responder" community, she said. This community, composed of police, firefighters, medical and rescue groups, etc., wants to have an ID that is compatible with the Federal ID card, e.g., PIV card. They point to the problems they encountered in trying to help at the Pentagon during the 9/11 attack. Fire and rescue could not get through the cordon to be able to reach the victims and fight the fires. Reportedly, a reporter dressed as a fireman breeched security and entered the cordoned off area.

Ms. Spencer reported there is another initiative within the financial community to build a first responder PKI bridge that will be cross-certified with the FBCA (it is assumed). They want to build a federal/industry PKI bridge for interoperable credentials within the financial industry for the first responder community.

b. ***SSP C&A Guidance***

Ms. Spencer said she is working as liaison for the GSA to DHS and is drafting a memo on what it takes to produce FIPS 201 compliant identity credentials. The GSA's chief concern is centered on identity proofing. She is arguing that the E-Authentication Guidance (NIST SP 800-63, combined with the FBCA CP Medium Hardware policy, have sufficient requirements (or the minimum standardized proofing that would be acceptable).

Before it is released, this memo will go to the Federal Identity Credentialing Committee (FICC) for comment, she said.

c. ***What it Means to be HSPD-12 "Compliant"***

Ms. Spencer said the memo she is drafting takes the position that if you issue a FIPS 201 compliant ID card, , e.g., one that conforms to NIST Guidance such as SP 800-63, etc., then you have the minimum credential that is compatible with the FBCA CP at Medium Hardware. In effect, you are cross-certified with the Federal Bridge at Medium Hardware. Ms. Spencer emphasized that the FIPS 201 PIV credential is equivalent to FBCA Medium Hardware.

The access decision will be made by the local system. You will always know the credential is "external." The cards in use by industry that purport to be HSPD-12 "comparable" are, in fact, HSPD-12 "Compatible." She noted that the CHUID and FASC-N are required to

authenticate the credential. We will have to develop a standardized FASC-N substitute to set the industry credentials apart, she said.

The implication of the credential on a card is that Medium Hardware is sufficient for authentication. Many of the SSPS vendors are planning to come in with commercial clones of their SSP services that they will cross-certify with the FBCA, she said.

d. ***October 11 2007 SSP Vendor Meeting***

Ms. Spencer said she is holding a meeting on October 11, 2007 with the SSP vendors to discuss the C&A process. We're trying to make sure we have common ground and understanding. She has commissioned a study of the methodologies used by the SSPs to certify and accredit their CAs. This is the process used before the NIST SP 800-53 process kicks in, she emphasized. The purpose of the study is to find out the compatibilities and similarities between the external PKI environment C&A process and that required for FISMA compliance. She said that NIST is working with her on this study. Many of the SSPs use the Web Trust methodology, she said.

Brian Dilley said that Microsoft is committed to supporting the new ISO 27118 International Audit standard, as well as ETSI and Web Trust.

ACTION: 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.

Agenda Item 7

Adjourn Meeting

The meeting adjourned at 10:40 a.m. The next FPKIPA meeting is scheduled for 13 November 2007 (9:30 a.m. – 11:30 a.m. at the USPS Headquarters, 475 L'Enfant Plaza, SW, Room 2P316 (inside 2P310), Washington, DC.

CURRENT ACTION ITEMS

No.	Action Statement	POC	Start Date	Target Date	Status
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, Rebecca Nielsen et al	11 July 2006	31 Jan. 2007	Open
259	Debbie Mitchell will forward policy statements to the FPKI PA for review when available.	Debbie Mitchell	12 Dec. 2006	9 Jan. 2007	Open
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
313	Dr. Alterman will contact each cross-certified member (who has not upgraded yet) to find out their strategy and whether or not they will be able to meet the October 27, 2007 deadline	Dr. Alterman	11 Sept. 2007	9 Oct. 2007	Open
314	Judy Fincher will contact Phil Welsh, the SAFE Technical POC, to see if any issues had arisen in SAFE's "reverse mode" testing.	Judy Fincher	9 Oct. 2007	19 Oct. 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
314	Dr. Alterman and Larry Shomo (DHS Contractor, Cygnacom) will talk offline next week to discuss DHS's plans for their PKI.	Dr. Alterman, Larry Shomo	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