Federal Public Key Infrastructure Policy Authority (FPKIPA)

Draft Minutes of the 11 March 2008 Meeting

USPS, 475 L'Enfant Plaza, SW, Washington, DC
Conference Room 2P316 (Inside 2P310)

A. AGENDA

1. Welcome / Introductions
2. Discussion / Vote on 12 February 2008 FPKIPA Minutes
3. FPKIPA Strategic Planning Committee
4. Discussion of new Operational Initiatives
    a. Document Management System (DMS)
    b. Flywheel
5. FPKI Certificate Policy Working Group (CPWG) Report
    a. Discuss/Vote on C4CP Change Proposal: 2008-01 (Aligning records archival requirements with NIST SP 800-63)
6. FPKI Management Authority (FPKI MA) Report
    a) Certificate Directory
    b) Cross-Certification Status
    c) Key Rollover Status
    d) Re-design Status
7. *Update on SSP and* SSPWG Activities
    a) SSP Quarterly Meeting
    b) Revised VeriSign CPS
    c) VeriSign SSP Clone
8. Final Meeting Items
    a. Other Topics:
        1. E-Vote to remove Wells Fargo Provisional Cross-Certification Status
        2. Presentation of Certificate of Appreciation
9. Adjourn Meeting

B. ATTENDANCE LIST

VOTING MEMBERS

The meeting began with a quorum of 11/15 (or 73%), where a two-thirds majority was required. This included four proxies (USPTO, Treasury, Commerce, and DHS). Another member joined the meeting after the quorum was established. Two alternates participated.

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

Organization	Name	Telephone
Department of Treasury	Proxy to HHS	
Drug Enforcement Administration (DEA CSOS)	ABSENT	
GPO	Hannan, John	
GSA - ALTERNATE	Spencer, Judith	
NASA -ALTERNATE	Levine, Susan	Teleconference
Nuclear Regulatory Commission- NRC	Sulser, David	
SSA	ABSENT	
USPS	Stepongzi, Mark	
USPTO	Proxy to HHS	

OBSERVERS

Organization	Name	Telephone
GSA	Jenkins, Cheryl	
SAFE	Cullen, Cindy	Teleconference
Wells Fargo	Drucker, Peri	Teleconference
FPKI/FICC Support (Contractor--General Dynamics Information Technology)	Petrick, Brant	
FPKIPA Secretariat (Contractor -- Protiviti Government Services)	Fincher, Judy	
FPKIPA (Contractor—Protiviti Government Services)	King, Matt	Teleconference
FPKI Management Authority (MA) Technical Lead (Contractor—Protiviti Government Services)	Brown, Wendy	
FPKI PA Support/Co-Chair CPWG (Contractor, Protiviti Government Services)	McBride, Terry	
MIT Lincoln Laboratory IT Security, ICS	Malabon, Mikiala	Teleconference
NASA	DeYoung, Dr. TIce	
DoS (Contractor, ManTech); Co-Chair, CPWG	Froehlich, Charles	
SSA (Contractor, Jacob and Sundstrom)	Simonetti, David	
KPMG	Faut, Nathan	

C. MEETING ACTIVITY

Agenda Item 1

Welcome / Introductions—Dr. Peter Alterman, Chair

The FPKIPA met at the USPS Headquarters Building located at 475 L'Enfant Plaza, SW, Washington, DC, in Conference Room 2P316 (inside 2P310). Dr. Peter Alterman, Chair, called the meeting to order at 9:40 a.m. The voting included four proxies: USPTO, Treasury, Commerce, and DHS, respectively, to HHS.

Agenda Item 2

Discussion / Vote on 12 February 2008 FPKIPA Minutes—Judy Fincher
Ms. Fincher said she incorporated all comments received and distributed a redline version of the minutes to the FPKIPA five working days prior to the 11 March 2008 FPKIPA meeting.

The FPKIPA voted by 11/15, or 73%, to approve the minutes, where a 50% majority was required.

Approval vote for 12 February FPKIPA Minutes – red line version			
Voting members	**Vote (Motion- NASA ; 2nd- USPS)**		
	Yes	**No**	**Abstain**
Department of Commerce (Proxy to HHS)			√
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 (Proxy to HHS)	√		
Drug Enforcement Administration (DEA CSOS)	Absent		
GPO	Absent for this vote only		
GSA	√		
NASA	√		
Nuclear Regulatory Commission	√		
SSA	Absent		
USPS	√		
USPTO (Proxy to HHS)	√		

Agenda Item 3

FPKIPA Strategic Planning Committee—Dr. Peter Alterman

Dr. Alterman said that GSA is moving to consolidate HSPD-12 and the E-Auth programs and also plans to roll FPKI into the new organization. Given that development, he felt it was appropriate to put a Working Group together regarding “Whither FPKI?”

Dr. Alterman said he would issue a call for participants in this Working Group. FICC Chair Judith Spencer will lead the group. He believes the WG will hold two-to-three hour-long teleconferences to brainstorm a Strategic Plan. Protiviti Government Services (formerly Enspier) will draft the Strategic Plan based on the findings of the Working Group.

Agenda Item 4

Discussion of new Operational Initiatives—Dr. Peter Alterman

a) Document Management System (DMS)

Dr. Alterman said that efforts have been underway for some time to create an on-line Document Management System or DMS. The DMS would be web –based and PKI enabled. The FPKIPA would use the DMS to distribute and manage documents under review, instead of relying on e-mail distribution.

Protiviti Government Services (PGS) has developed a prototype system. Terry McBride of PGS is developing a functional specification for purchase of the server and other equipment. Dr. Alterman has not yet decided where the DMS will be located: possibly at HHS, GSA or PGS.

Judith Spencer said she wanted everybody to be using PIV cards to access the system by early next year. In the interim, Dr. Alterman plans to purchase digital certificates for those who do not have them yet.

ACTION: Judy Fincher is to get from Cheryl Jenkins the information on Identrust ACES business certificates and their voucher program.

b) Flywheel

Dr, Alterman said he is borrowing from Internet2 the concept of a flywheel and is implementing it within the FPKIPA. He wants a single point of contact to track the progress of each applicant PKI or SSP Candidate, like what Matt King has been doing for the University of Texas and Wells Fargo for the past 6-9 months. PGS have identified people to do this for each entity that wishes to become an SSP and/or become cross-certified with the FBCA.

Agenda Item 5

FPKI Certificate Policy Working Group (CPWG) Report—Judith Spencer

Dr. Alterman asked Judith Spencer to give the CPWG Report in Dave Cooper's absence. Dr. Alterman said that Dave Cooper has resigned as Co-Chair of the CPWG, but will remain as a technical advisor. Shortly after the meeting, Dr. Alterman announced via e-mail that Charles Froehlich (DoS Contractor and PKI Policy wonk) and Terry McBride, a PKI technical expert from PGS, would serve as Co-Chairs. John Cornell will step aside to become the official Legal Advisor to the CPWG.

a. Discuss/Vote on C4CP Change Proposal: 2008-01 (Aligning records archival requirements with NIST SP 800-63)

Judith Spencer said the importance of this Change Proposal is that it aligns C4 with the archival requirements in NIST SP 800-63, since E-Auth Level 2 requirements are satisfied by C4.

There was some discussion as to whether this vote should be postponed until the Archive Working Group meets later today. John Hannan said that the archives group is focused on E-Auth Level 3 requirements. Cheryl Jenkins wanted to move forward on the C4CP Change Proposal to address 800-63 requirements. Dr, Alterman concurred. Whatever changes made to the FBCA CP will not affect this Change Proposal, he said.

The FPKIPA then voted by 13/15 or 86.7% of eligible voters, to approve the C4CP Change Proposal: 2008-01, where a 75% majority vote was required.

Approval vote on C4CP Change Proposal: 2008-01 (aligning records archival requirements with NIST SP 800-63)			
Voting members	**Vote (Motion – NRC ; 2nd – DoS)**		
	Yes	**No**	**Abstain**
Department of Commerce (Proxy to HHS)	√		
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 (Proxy to HHS)	√		
Drug Enforcement Administration (DEA CSOS)	Absent		
GPO	√		
GSA	√		
NASA	√		
Nuclear Regulatory Commission	√		
SSA	Absent		
USPS	√		
USPTO ((Proxy to HHS)	√		

Agenda Item 6

FPKI Management Authority (FPKI MA) Report—Cheryl Jenkins

a. Certificate Directory Status

The FPKI Operational Authority has come under GSA/FAS management and is now known as the FPKI Management Authority (FPKI MA). There are numerous issues with the FBCA Directory, Ms. Jenkins said, adding that the FPKI MA intends to sunset X.500 chaining at the end of this year as part of the FPKIA re-design. If this affects you, let us know, she said.

Ms. Jenkins said she will post color-coded “score cards” on the FPKI MA website so that entities may review outstanding directory issues, as well as successes. The FPKI MA will issue the January-February report in the March 15-18 timeframe, she said. These scores tie back to policy compliance issues

b. Cross Certification Status

The MIT LL Mapping is completed but changes in the FPKIA Directory schema are required in order to successfully chain to the MIT LL Directory. This needs to happen before the FPKI MA can post their certificate. This will happen soon.

DHS and NASA are moving under the SSP program. Revocation of the NASA certificates should occur by the end of March. The MA is waiting for notice of when the DHS move will occur.

There is a discrepancy in the Wells Fargo directory, she reported.

ACTION: Cheryl Jenkins and Dr. Peter Alterman will reach out to Wells Fargo to determine what should be in the Directory and what the next steps are.

Ms. Jenkins also met with DoD to get their certificates back into the Directory. The FPKI MA performed the directory interoperability testing and discovered an issue in the DoD LDAP Directory. DoD has submitted a plan to provide data to correct the issue and Ms. Jenkins is looking at the DoD plan today.

c. Key Rollover Status

The FPKI MA performed three key rollovers: the e-Governance CA, the Common Policy CA, and the FBCA, Ms. Jenkins reported. We are also about to roll over the C4CA, she said.

Ms. Jenkins is sending emails showing the prioritization of signing the new certificates that are required. The FPKI MA will deal with requests in the order received. She noted that IdenTrust (ACES). DoS and DEA needed to follow up with plans for receiving their new certificate, following the FBCA Key Rollover.

d. Re-design Status

The FPKI MA received funding for the IV&V yesterday and the contract will be awarded next week to A&N.

The implementation plan is now is its second revision. A&N will be reviewing it for business and technical drivers required to support HSPD-12.

The plan is to have the re-designed system up and running by the end of December 2008.

Agenda Item 7

Update on SSP and SSPWG Activities—Judith Spencer

a. SSP Quarterly Meeting

Ms. Spencer is planning to hold the quarterly meeting with the SSPs in April. Dave Cooper will brief the SSPs on directory issues and Richard Wilshire will brief the SSPs on the evaluation he performed on industry C&A processes, which he mapped back to NIST SP 800-53.

Ms. Spencer and Dr. Peter Alterman will review Mr. Wilshire's findings and distribute it to the FPKIPA. Mr. Wilshire identified several "alarm bells" such as what appears to be the violation of the auditor role. Various SSP auditors recommended solutions to address the vulnerabilities found in the C&A process. External auditors should not make suggestions because that is a conflict of interest. Ms. Spencer checked with Marianne Swanson of NIST who concurred that this is a violation of the auditor role. The issue is the independence of the third party auditor.

It is okay to fix vulnerabilities before the auditor issues the final report and it has been traditional for C&A evaluators to make recommendations on how to fix security problems, not necessarily PKI-related. Ms. Jenkins concurred. Certifying Officials are part of your team, i.e., to help you fix problems.

NIST SP 800-37 is under revision and this issue should be on the list of things to be clarified. It is a question of the independence of the auditor versus the role of the C&A security consultant.

Nathan Faut (KPMG) suggested that security consultants can set up compensating controls, rather than making the fix.

Cheryl Jenkins said the recommendations are high-level guidance; they are not directions on how to make the fix.

Dr. Peter Alterman said it is a fine line between the two activities and context is what is important. He referred to a saying of John Cornell: it is the shading of things. This should not be a problem if you are clear in the contract and in the SOW agreement, he said. In addition, he added, NIST will inform us as to what we should do.

b. Revised VeriSign CPS

Ms. Spencer said that she distributed the revised VeriSign CPS to the SSPWG last week for review and discussed it with Nick Piazzola, the VeriSIgn SSP POC. She anticipates one more round with the SSPWG via e-mail before VeriSign is approved at Common High.

c. VeriSign SSP Clone

Ms. Spencer said that VeriSign wishes to cross certify their commercial SSP clone with the Federal Bridge at all levels of assurance. VeriSign anticipates having state and local government customers, so that Bridge "High" is appropriate. Note: It is reserved for "government agencies only." Many state and local governments are buying from commercial SSPs. They want to sell Medium Hardware credentials to state governments and others who want to be HSPD-12 compatible. It is a peer-to-peer relationship. SSPs can only sell to federal government agencies. The FICC in cooperation with OMB is defining "HSPD-12 clone." Entities in a trust relationship with the Federal Bridge will be HSPD-12 compliant, she added.

Ms. Spencer said that the document, "Interoperability Parameters for Trusting PIV Compatible Identity Cards," is almost ready for FICC release and that she is working closely with Tom Lockwood of DHS who needs it now to support the activities run by the states that make use of PIV-like card capabilities, such as ACIS, FRAC and TWIC.

Debbie Mitchell wanted to know if the FICC would approve the document referenced above before VeriSign comes in as a Common Policy clone for cross-certification.

Ms. Spencer said it would not, but that the issue here is “compatibility,” not compliance.

Agenda Item 8

Final Meeting Items

a. Other Topics:

1. E-vote to remove Wells Fargo Provisional Cross-Certification Status
   Dr. Alterman said Wells Fargo had been “Provisional” (at Basic) until their HSM was FIPS 140 compliant. This will occur the end of March 2008.

   ACTION: Ms. Fincher will issue an e-vote the last week of March 2008 to ask the FPKIPA to vote to remove the provisional status of the Wells Fargo cross-certification.

2. Presentation of Certificate of Appreciation
   Dr. Alterman presented a certificate of appreciation to Dr. Tice DeYoung who is retiring the end of March 2008 from NASA. Consequently, he has relinquished his long-standing representation on the FPKI Policy Authority.

Agenda Item 9

Adjourn Meeting

Dr. Alterman adjourned the meeting at 10:47 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
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

No.	Action Statement	POC	Start Date	Target Date	Status
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
327	Cheryl Jenkins will send the annotated Implementation Plan to Judy Fincher for distribution to all cross-certified members of the FPKIPA.	Cheryl Jenkins	11 Dec. 2007	January 2008	Open
328	Judy Fincher is to get from Cheryl Jenkins the information on Identrust ACES business certificates and their voucher program	Judy Fincher	11 March 2008	21 March 2008	Open
329	Cheryl Jenkins and Dr. Peter Alterman will reach out to Wells Fargo to determine what should be in the Directory and what the next steps are.	Cheryl Jenkins, Dr. Peter Alterman	11 March 2008	21 March 2008	Open
330	Ms. Fincher will issue an e-vote the last week of March 2008 to ask the FPKIPA to vote to remove the provisional status of the Wells Fargo cross-certification.	Judy Fincher	11 March 2008	21 March 2008	Open