Minutes of the 12 August 2008 Meeting

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

A. AGENDA

1. Welcome / Introductions
2. Re-organization of the Office of Governmentwide Policy
3. Discussion / Vote on 10 June 2008 FPKIPA Minutes
4. Discussion / Vote on 8 July 2008 FPKIPA Minutes
5. Results of three e-votes (auditor independence, archiving)
6. FPKI Certificate Policy Working Group (CPWG) Report
    a. CPWG Recommendation to accept the DoS Audit Letters for their 5 CAs
    b. Discuss need for a new FBCA CP Change Proposal
    c. Status report on Mapping DoD ECA (one-way) at Medium Hardware
    d. Discuss CPWG Recommendation to accept the Wells Fargo Audit
    e. Status report on Mapping VeriSign non-fed SSP CA "Clone" at Rudimentary, Basic, Medium, Medium Hardware and High
7. Discussion of the Viability of Cross—certifying non-fed SSP PKI "Clones" at the High Assurance Level
8. FPKI Management Authority (FPKI MA) Report
9. Final Meeting Items
    a. Other Topics
    b. Proposed Agenda Items for the next FPKIPA meeting, 9 September 2008
        1. Discuss Cross Certification of non-fed SSP CA Cross-certified "clones" at High
        2. Results of e-vote to accept the Wells Fargo WebTrust Audit
        3. Clarification from DoD on whether DoD ECA certs will be one-way or two-way cross-certified
        4. FPKIPA Action Item review (please scrub this list BEFORE the 9 September 2008 FPKIPA meeting)
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. Commerce joined the call in progress and did not participate in any of the votes, making the attendance 13/15. USPTO and SSA were absent.

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@pgs.protiviti.com.

Organization	Name	Telephone
Department of Commerce (NIST)	Cooper, Dave	Teleconference
Department of Defense	Mitchell, Debbie	Teleconference
Department of Health & Human Services	Proxy to GSA	
Department of Homeland Security	Hagerling, Don	
Department of Justice	Morrison, Scott	
Department of State	McCloy, Mark A.	
Department of Treasury	Schminky, Jim	
Drug Enforcement Administration (DEA CSOS)	Jewell, Chris	Teleconference
GPO	Hannan, John	Teleconference
GSA	Alterman, Dr. Peter	
NASA -Alternate	Levine, Susan	Teleconference
Nuclear Regulatory Commission- NRC	Sulser, David	
SSA	Absent	
USPS	Stepongzi, Mark	
USPTO	Absent	

OBSERVERS

Organization	Name	Telephone
FPKIPA Acting Chair, FICC Chair / GSA	Spencer, Judith	
FPKI Management Authority (MA)/GSA	Jenkins, Cheryl	Teleconference
State of Illinois	Anderson, Mark	Teleconference
NOAA (Contractor, General Dynamics)	Wright, Bill	
KPMG	Faut, Nathan	Teleconference
Department of State/ Co-chair, CPWG (Contractor, ManTech)	Froehlich, Charles	
Wells Fargo	Gross, Jim	Teleconference
Wells Fargo	Drucker, Peri	Teleconference
Treasury	Robinson, Michael	
FPKI/FICC Support (Contractor--FC Business Systems LLC)	Petrick, Brant	
FPKIPA Secretariat (Contractor -- Protiviti Government Services)	Fincher, Judy	
FPKI PA Support/Co-Chair CPWG (Contractor, Protiviti Government Services)	McBride, Terry	
eValid8	Dilley, Brian	

C. MEETING ACTIVITY

Agenda Item 1

Welcome / Introductions—Ms. Judith Spencer, Interim Chair

The FPKIPA met at the USPS Headquarters Building located at 475 L'Enfant Plaza, SW, Washington, DC, in Conference Room 2P316 (inside 2P310). Ms. Judith Spencer, Interim Chair, called the meeting to order at 9:39 a.m.

Dr. Peter Alterman, Out-going Chair, stated that he had resigned to take the position of Deputy Associate Administrator (DAA) for Technology Strategy, Office of Governmentwide Policy, General Services Administration (GSA), effective August 1, 2008. He said that the Charter calls for election of a new Chair within 30 days of the resignation of a standing Chair, in an emergency situation, and that this situation meets that definition. However, because the OGP is being re-organized, it would not be fair to ask anyone to assume the permanent Chair position until the positions' job description is known. Therefore, Ms. Spencer (FICC Chair, who reports directly to Dr. Alterman), will assume the position of Interim Chair for the next 60 days. By the end of FY 08, the new organization should be in place and the Charter of the FPKIPA, defined. At that time, the FPKIPA, acting under its new Charter, would be in a position to elect a new Chair.

We wish to thank Mr. Mark Stepongzi for his hospitality in providing the room and audio-visual facilities.

Agenda Item 2

Re-organization of the Office of Governmentwide Policy—Dr. Peter Alterman, Ms. Judith Spencer

Dr. Alterman said that the OMB Identity Management (IdM) Portfolio Manager (Ms. Carol Bales) is working with the CIO Council to re-define the role of the FPKI Policy Authority, in light of the creation of an IdM PMO. Dr. Alterman assured the FPKIPA members that the Policy Authority would continue to play a necessary and useful role in the re-organized OGP.

Dr. Alterman will take on the government-wide OGP collaboration of Federal IdM in his role as DAA of the Office of Technology Strategy. The goal is to institutionalize the FPKIPA and FPKI MA within GSA OGP so that they will be less of a target when the new administration comes in. They, along with the E-Auth PMO, are among the four or five of the 25+ e-gov initiatives that have not "graduated." This is a thing from this administration until we get it institutionalized to protect it, Ms. Spencer said.

This will result in more adequate funding for the MA and a continued life for the FPKIPA, but apparently, not for the E-Auth PMO, as we know it. FAS will no longer be running the E-Auth Federation; the OGP will run it, using a "more open architecture," infrastructure changes and a new business model. Ms. Spencer noted that there is "lots of maturity" in the marketplace, e.g., SAML 2 products. The E-Auth concept is good and encompasses both Fed PKI and HSPD-12, which are viewed by OMB as "tools, not initiatives." Existing SAML projects will be transitioned to scheduled services. There will be no requirement to buy a specific solution from a specific vendor.

For example, the Managed Validation Translation Service (MVTS) might be kept, but not as a centralized service supported by all the agencies. It would be run by FAS as a cost-reimbursable program and would be optional. Agencies would not be required to use the services of any one vendor, for example. Satisfying M-04-04, the Foreman memo and SP 800-63 is the goal. How you get there is up to you.

GSA will get the agencies to work together using a yet TBD distributed model, under the mandate of the Mark Foreman (2003) OMB memo: all agencies are urged to "play together in the same sandbox." The Federal Identity Credentialing Committee (FICC) will be the "gathering place" going forward to get the agencies to play together, Dr. Alterman said.

Jim Schminky asked about the continued financial viability of the FPKI MA. Dr. Alterman said that since OGP is the only appropriated office in GSA, he is working with OMB on that. This will not affect the Fed PKI, he said. The MA should be able to start buying equipment for the FPKIA re-design within 3 months, Ms. Spencer said.

Mark McCloy asked if the re-organization is a threat to legacy PKIs. Dr. Alterman said there has been no "push back" on the conceptual model for FPKI, and Ms. Spencer stressed that Fed PKI is the model for turning E-Auth around.

The FPKIPA agreed to hold off on discussing the election of the new Chair until the picture is clearer.

Agenda Item 3

Discussion / Vote on 10 June 2008 FPKIPA Minutes—Judy Fincher

Ms. Fincher said she incorporated all the comments received on the 10 June 2008 FPKIPA minutes and displayed the comments on the LCD projector. The FPKIPA voted unanimously (12/12) to approve the minutes, as amended. Commerce, USPTO and SSA were absent for this vote. DHS moved the motion and Treasury seconded.

Agenda Item 4

Discussion / Vote on the 8 July 2008 FPKIPA Minutes—Judy Fincher

Ms. Fincher said she incorporated all the comments received on the 8 July 2008 FPKIPA minutes and displayed the comments on the LCD projector. The FPKIPA voted unanimously (12/12) to approve the minutes, as amended. Commerce, USPTO and SSA were absent for this vote. DHS moved the motion and Treasury seconded.

Agenda Item 5

Results of three e-votes (auditor independence, archiving)—Judy Fincher

This item was not reported in the meeting, but was communicated in an email to the FPKIPA listserv on July 25, 2008 12:03 p.m.

The e-votes to approve the three Change Proposals were successful. All three e–votes passed by 13/15 (86.7%) of voting members, where a 75% majority vote was required. The following agencies voted, "Yes:" DoS, HHS, DEA CSOS, DOJ, SSA, GPO, USPS, NRC, NASA, Treasury, DHS and GSA. Commerce and USPTO did not vote.

The items voted on were:
FBCA CP Change Proposal: 2008-02 (archiving)
FBCA CP Change Proposal: 2008-03 (auditor independence)
Common CP Change Proposal: 2008-01 (auditor independence)

Agenda Item 6

FPKI Certificate Policy Working Group (CPWG) Report—Charles Froehlich, Terry McBride

a. CPWG Recommendation to accept the DoS Audit Letters for their 5 CAs
Ms. Fincher displayed the CPWG recommendation to accept the DoS Audit Letters for their five CAs and the FPKIPA accepted the recommendation.

b. Discuss need for a new FBCA CP Change Proposal
Charles Froehlich said his Crits and Methods Change Proposal is being transitioned into a FBCA CP Change Proposal and that it will be presented at the August 19 meeting of the CPWG. This is needed to correct language in the FBCA related to who may assert the "High" assurance level.

c. Status report on Mapping DoD ECA (one-way) at Medium Hardware
Terry McBride reported that the CPWG at the 7 August CPWG meeting finished mapping DoD ECA, but that there were several minor issues remaining. The edited CP and tables will be reviewed at the 19 August CPWG meeting. Ms. Mitchell said she would check to see if it would be a one-way or two-way mapping and report back at the 9 September meeting.

d. Discuss CPWG Recommendation to accept the Wells Fargo Audit
Terry McBride read excerpts from the Wells Fargo WebTrust audit letter prepared by KPMG. The chief remaining issue was the phrase, "based on the WebTrust criteria." Several CPWG members did not feel that the WebTrust Criteria were sufficiently attuned to the FPKIPA requirements to be acceptable. In particular, John Cornell did not feel the verbiage of the standard Web Trust audit letter adequately addresses the changing requirements of the "Audit Cookbook." Furthermore, making changes to the Web Trust Audit Criteria will require it to be evaluated and processed by the AICPA, which will be time-consuming.

The CPWG issued a recommendation to the FPKIPA to accept the Wells Fargo Audit, although it was not collectively recommended. The rationale was that the risk of accepting the Wells Fargo audit is "extremely low." Wells Fargo has not issued any certificates against this CA and Wells Fargo will begin a new audit cycle in two months. Wells Fargo will present the new audit letter in early 2009, according to Jim Gross. Furthermore, WebTrust for CAs is the industry standard. We have accepted

many WebTrust audits in the past and why should *ex post facto* requirements be levied on Wells Fargo when they had not been on the others, Ms. Spencer said. The audit requirements are a moving target and Wells Fargo is being penalized for having submitted its documentation when other rules were in effect.

DoD (Debbie Mitchell) was concerned that the older CPS was weak and that a new CPS is needed. Peri Drucker (Wells Fargo) said Wells Fargo had changed the CPS in November 2007 to incorporate stronger business practices and reiterated that they had not issued any certificates.

Jim Schminky moved that the FPKIPA vote to accept the CPWG audit recommendation for Wells Fargo. Dave Cooper objected to the vote on procedural grounds. He said the By-Laws did not permit votes unless members were notified five business days in advance that a vote would occur. It was agreed that the FPKIPA Secretariat would issue an e-vote on accepting the Wells Fargo Audit Letter at least five business days after the 12 August FPKIPA meeting.

e. Status report on Mapping VeriSign non-fed SSP CA "Clone" at Rudimentary, Basic, Medium, Medium Hardware and High

Terry McBride said the VeriSign non-fed SSP CA "Clone" General matrix has been reviewed by the CPWG and that there were some issues. As a result, the CPWG referred it back to VeriSign for clarification.

Agenda Item 7

Discussion of the Viability of Cross-certifying non-fed SSP PKI "Clones" at the High Assurance Level

Two commercial SSPs (VeriSign and Verizon Business) want to come in at the "High" assurance level. The issue is, Jim Schminky asked, do we want SSPs to issue cross certs with the Bridge at High?

Ms. Spencer said that this request to do business in our sphere, on our behalf, is mostly related to HSPD-12. She, as FICC Chair, asked SSP commercial vendors to cross-certify a clone of their commercial service so that they can offer certs to external entities, e.g., industry, state and local governments, etc. Certain key DHS-related programs such as FRAC, TWIC and ACIS need cards that are interoperable with PIV cards.

Under the Common Policy, we have commercial SSPs that can issue certificates at Common High to Federal agencies (only). However, COMMON credentials (OIDS) cannot be issued outside the Federal Government. We need a solution. Everyone knows the story of Arlington County fire fighters being turned away on 9/11 from the Pentagon fire because they did not have the right credentials, e.g., a CAC card.

The FBCA CP says that states, local governments and tribal entities can also issue at High. Clones need to be cross-certified at High for interoperability at High with Federal agencies, local and state governments, and tribal entities.

GSA does a FISMA C&A on all SSPs, but would not require a C&A on clones, e.g., VeriSign and Verizon Business.

David Sulser said that NRC had done a C&A on the VeriSign clone, and verified that it runs on the same infrastructure as the SSP that has the C&A from GSA. Since 1998, NRC has issued certs to external stakeholders that do not fall under the affiliate PIV definition. Most get Medium Hardware.

Some FPKIPA members contended that High must be reserved for governments. The State of Pennsylvania has First Responder entities who will get FRAC cards. They want a credential policy with FRAC cards at High assurance.

We would need assurances in their MOAs concerning this and their documentation have to clearly delineate how they are going to control it to make sure they do not violate policy, Ms. Spencer said. Or, Dr. Alterman said, the FPKIPA could choose to say only governments can get "High" certificates. The implication would be that the FRAC communities would have to stand up their own CAs. He also said that we cannot modify COMMON (SSP Program) to bring states under Federal Control due to statutory regulations, e.g., states rights, etc.

The FPKIPA decided to continue this discussion next month at the 9 September FPKIPA.

Agenda Item 8

FPKI Management Authority (FPKI MA) Report—Cheryl Jenkins

1- Ms. Jenkins said that a Work Package is in the works that deals with technology change related to the use of SHA-256. The recommendation will be to accept certs requiring SHA-256, but to sign with SHA-1 until 2010.
2- Ms. Jenkins also said she was working on a Change Proposal on how to make technology refreshment changes to policy.
3- Regarding the FPKIA re-design, Ms. Jenkins said the MA may move to another Directory product as more issues are identified with the existing vendor, ISODE, as new members come on board. In the meantime, we need to roll out repositories all over before we are hit by a high volume of traffic. Our goal is 99.9% availability.

Agenda Item 9

Final Meeting Items

a. Other Topics

1) Need for test OID for COMMON---Judith Spencer said she would be submitting a Change Proposal on adding a test OID for COMMON to the CPWG at its Aug. 19, 2008 meeting. The problem is that we cannot issue test cards to the vendor community who want to test their cards with HSPD-12 credentials. They cannot chain back to the hierarchical root.

2) Proposed Agenda Items for the next FPKIPA meeting, 9 September 2008

1. Discuss Cross Certification of non-fed SSP CA Cross-certified "clones" at High
2. Results of e-vote to accept the Wells Fargo WebTrust Audit
3. Clarification from DoD on whether DoD ECA certs will be one-way or two-way cross-certified
4. FPKIPA Action Item review (please scrub this list BEFORE the 9 September 2008 FPKIPA meeting)

Action Item 10

Adjourn Meeting

Ms. Spencer adjourned the meeting at 11:30 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
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
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
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

No.	Action Statement	POC	Start Date	Target Date	Status
331	Dr. Alterman will draft language for the FBCA policy change procedure to do some "reality testing" and distribute it to the FPKIPA.	Dr. Peter Alterman	8 April 2008	13 May 2008	Open
366	Debbie Mitchell will share the finalized DoD Test Plan; the FPKIPA will then review it and decide what pieces they can and cannot do. Then Cheryl Jenkins will follow up to make sure the test plan includes testing at the application level,--not just the PKI level.	Debbie Mitchell, FPKIPA, Cheryl Jenkins	13 May 2008	10 June 2008	Open
371	Dr. Alterman will inform Verizon Business Systems (VBS) that their application was approved and will ask for the ETA for the Policy.	Dr. Peter Alterman	8 July 2008	15 July 2008	Open