FPKIPA
Federal Public Key Infrastructure Policy Authority

Minutes of the 8 July 2008 Meeting

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

A. AGENDA

1. Welcome / Introductions
2. Discussion / Vote on 10 June 2008 FPKIPA Minutes
3. Results of the e-vote to Cross-Certify Wells Fargo (new CA) at Medium, Medium Hardware, Medium CBP and Medium Hardware CBP
4. Discuss/Vote to accept Verizon Business (CyberTrust) Application for Cross-Certification with the FBCA
5. Discuss revocation of the MIT Lincoln Laboratory cross-certification
6. Report on the Forum of the Four Bridges
7. FPKI Certificate Policy Working Group (CPWG) Report
   a. Discuss/Vote to accept FBCA CP Change Proposal: 2008-02 (archiving)
   b. Discuss/Vote to accept FBCA CP Change Proposal: 2008-03 (Auditor Independence)
   c. Discuss/Vote to accept Common Policy Change Proposal: 2008-01 (Auditor Independence)
   d. Discuss the Status of the Wells Fargo Audit and Cross-Certification
8. FPKI Management Authority (FPKI MA) Report
9. *Update on SSP and* SSPWG Activities
10. Final Meeting Items
    a. Other Topics
    b. Proposed Agenda Items for the next FPKIPA meeting, 12 August 2008. Results of three e-votes:
       1. Discuss/Vote to accept FBCA CP Change Proposal: 2008-02 (archiving)
       2. Discuss/Vote to accept FBCA CP Change Proposal: 2008-03 (Auditor Independence)
       3. Discuss/Vote to accept Common Policy Change Proposal: 2008-01A (Auditor Independence)
    c. FPKIPA Action Item review (please scrub this list BEFORE the 12 August 2008 FPKIPA meeting)
11. 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.

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	
Department of Health & Human Services	Alterman, Dr. Peter	
Department of Homeland Security - proxy to HHS	Proxy to HHS	
Department of Justice	Morrison, Scott	
Department of State	McCloy, Mark A.	
Department of Treasury	Absent	
Drug Enforcement Administration (DEA CSOS)	Absent	
GPO	Hannan, John	Teleconference
GSA	Spencer, Judith	
NASA -Alternate	Absent	
Nuclear Regulatory Commission- NRC	Sulser, David	
SSA	Mitchell, Eric	Teleconference
USPS	Stepongzi, Mark	
USPTO	Absent	

OBSERVERS

Organization	Name	Telephone
FPKI Management Authority (MA)/GSA	Jenkins, Cheryl	Teleconference
KPMG (Chair, WebTrust of AICPA)	Lundin, Mark	Teleconference
NOAA (Contractor, General Dynamics)	Wright, Bill	301-713-7087
IdenTrust	Schambach, Marco	Teleconference
Department of State/ Co-chair, CPWG (Contractor, ManTech)	Froehlich, Charles	
Wells Fargo	Gross, Jim	Teleconference
Wells Fargo	Drucker, Peri	Teleconference
GSA (Legal Counsel)	Cornell, John	Teleconference
FPKI/FICC Support (Contractor--FC Business Systems LLC)	Petrick, Brant	
FPKIPA Secretariat (Contractor -- Protiviti Government Services)	Fincher, Judy	
EPA (Contractor, Jacob & Sundstrom)	Simonetti, David	Teleconference
SSA (Contractor, Jacob & Sundstrom)	Jackmon, Kenya	
FPKI Management Authority (MA) Technical Lead (Contractor—Protiviti Government Services)	Brown, Wendy	
FPKI PA Support/Co-Chair CPWG (Contractor, Protiviti Government Services)	McBride, Terry	

Organization	Name	Telephone
FPKIPA Support (Contractor, Protiviti Government Services)	King, Matt	

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). The Chair, called the meeting to order at 9:35 a.m.

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

Agenda Item 2

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. She distributed the redline version along with the agenda and meeting notice five business days prior to the 8 July 2008 meeting. Debbie Mitchell said her comments had not been included. Ms. Fincher will add the two paragraphs and distribute the revised final draft of the minutes to the FPKIPA for a vote at the 12 August FPKIPA. (Done)

Agenda Item 3

Results of the e-vote to cross-certify Wells Fargo (new CA) at Medium, Medium Hardware, Medium CBP and Medium Hardware CBP

Ms. Fincher said the e-vote to cross-certify Wells Fargo at Medium, Medium Hardware, Medium CBP and Medium Hardware CBP did not pass.

Results of the E- Vote on Cross-Certification with Wells Fargo at Medium, Medium Hardware, Medium CBP, and Medium Hardware CBP			
Voting members			
	Yes	**No**	**Abstain**
Department of Commerce		√	
Department of Defense		√	
Department of Health & Human Services	√		
Department of Homeland Security	DID NOT VOTE		
Department of Justice		√	
Department of State	√		

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

Agenda Item 4

Discuss/Vote to accept Verizon Business (CyberTrust) Application for Cross-Certification with the FBCA—Dr. Peter Alterman, John Cornell, Judith Spencer

Verizon Business Systems submitted an application for cross-certification of their CA with the Federal Bridge at all assurance levels except Rudimentary. Ms. Spencer said that GSA was the sponsoring agency. The Federal interest in this cross-certification is two-fold, she said:

1- Provide compatible PIV credentials, e.g., interoperable cards, to entities external to the Federal Government, such as the First Responder community, state governments, and industry sectors.
2- Leverage their work in the E-Auth space.

Ms. Spencer said the FICC Governance Working Group is writing guidance on extra-federal interoperability. This guidance, currently called "Interoperability Parameters [Requirements] for Trusting PIV Compatible Identity Cards", will require cross-certification of the providers of these services with the Federal Bridge at Medium Hardware or High. These cards would not be FIPS 201 "compliant," but would be considered FIPS 201 compatible. The cards could be read in the native reader already installed at the agencies. Service providers may issue interoperable credentials, but it is up to the local agency to decide whether or not to trust those credentials.

The measure passed by 10/11 or 90.9% of votes cast where Majority of votes cast was required.

Vote to accept the Verizon Business (CyberTrust) Application for Cross-Certification with the FBCA			
Voting members	**Vote (Motion – NRC ; 2nd – USPS)**		
	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	ABSENT		
Drug Enforcement Administration (DEA CSOS)	ABSENT		
GPO	√		
GSA	√		
NASA	ABSENT		
Nuclear Regulatory Commission (NRC)	√		
SSA	√		
USPS	√		
USPTO	ABSENT		

ACTION: Dr. Alterman will inform Verizon Business Systems (VBS) that their application was approved and will ask for the ETA for the Policy.

Agenda Item 5

Discuss revocation of the MIT Lincoln Laboratory cross-certification—Dr. Peter Alterman

MIT Lincoln Laboratory sent a letter to Dr. Alterman informing him of their decision to withdraw from the FPKIPA. Due to resource reasons, MIT Lincoln Laboratory is unable to fulfill the requirements of the MOA.

The FPKIPA then discussed whether a vote to revoke the cross certificate was required. It is not explicitly called out in the Charter but is implied in the voting table. The FPKIPA agreed that since we have an authenticated request on MIT Lincoln Laboratory letterhead stationary, and the Chair verified the request on the back-end, there was no need to vote.

Cheryl Jenkins said she would accept the letter from MIT Lincoln Laboratory as a request to revoke the certificate and would verify it as well. The FPKI MA team will notify MIT Lincoln Laboratory when the cross certificate is revoked and report back to the FPKIPA.

Agenda Item 6

Report on the Forum of the Four Bridges—Dr. Peter Alterman

Dr. Alterman said that representatives from the four bridges (SAFE, FBCA, CertiPath and HEBCA) met in Linthicum, MD, on June 13 to discuss issues of interest to the bridges, such as operations, audits, outreach and PKI-enabled, interoperable applications. Wendy Brown represented the FPKI MA. On 21 August 2008, the Forum will meet with the auditor community to continue these discussions. Dr. Alterman emphasized that the Bridge operators cannot assure the qualifications and competence of individual auditors and sees that as the responsibility of the audit industry.

There is also an initiative underway to host a major PR event in the spring of 2009. A work team has been set up, and Tim Pinegar of PGS is representing the FPKIPA.

Mark Lundin, the chair of the WebTrust committee of the AICPA, will participate in the 15 July 2008 CPWG meeting to discuss the WebTrust methodology and invited feedback.

Agenda Item 7

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

a. Discuss/Vote to accept FBCA CP Change Proposal: 2008-02 (archiving)

   Terry McBride introduced the proposed FBCA CP Change Proposal: 2008-02 (archiving). He said he had made four changes:

   1. Reduced the number of events to be audited
   2. Added a reference to NARA to remind Federal Government agencies that they have to follow NARA records management and retention schedules
   3. Clarified the types of auditable events
   4. Added a list of archival events.

   Based on the lack of a voting quorum for this action, it was decided to hold an e-vote due in two weeks (COB Thursday 24 July 2008) so that members who could not attend the 8 July 2008 meeting because of vacation schedules could participate.

b. Discuss/Vote to accept FBCA CP Change Proposal: 2008-03 (Auditor Independence)

   This Change Proposal was not discussed. The FPKIPA decided to hold an e-vote due in two weeks (COB Thursday 24 July 2008) so that members who could not attend the 8 July 2008 meeting because of vacation schedules could participate.

c. Discuss/Vote to accept Common Policy Change Proposal: 2008-01A (Auditor Independence)

This Change Proposal was not discussed. The FPKIPA decided to hold an e-vote due in two weeks (COB Thursday 24 July 2008) so that members who could not attend the 8 July 2008 meeting because of vacation schedules could participate.

d. Discuss the Status of the Wells Fargo Audit and Cross-Certification

Dr. Alterman summarized the steps taken after the e-vote to cross certify Wells Fargo failed. He said that all five of David Temoshok's points (as captured in the June 10 2008 minutes) were being addressed and apologized for calling for an e-vote until the CPWG was satisfied with the result.

Wells Fargo representatives joined the discussion, as did the KPMG lead auditor for Wells Fargo (Mark Lundin), to discuss the adequacy, coverage and appropriateness of WebTrust as a PKI audit methodology. Wells Fargo (Peri Drucker) stated that they had followed the guidance in place when the audit began. She said the Wells Fargo audit performed in November 1 2006 through October 31, 2007 was done against the year before and as such, reflected a particular instantiation of Wells Fargo's practices at that time. John Cornell had reservations about whether WebTrust addresses all the ”shall” statements in the CPS. He counted 130 areas of inquiry in the standard WebTrust audit, but found over 540 “shall” statements in the CPS 3647-format. He said he did not have enough information to assert that the WebTrust audit was looking at everything the CPS requires, nor could he say it did not.

Dr. Alterman stated that the Policy Authority could agree that there were only a few minor things keeping the Wells Fargo audit from being acceptable and that the gap between the audit that Wells Fargo submitted and the FBCA's requirement was narrow.

DoD (Debbie Mitchell) said that she did not feel she could support Dr. Alterman's statement. She said that her technical experts who been attending the CPWG where the Wells Fargo Audit has been discussed over several months were not present at the PA meeting today. She had reservations about the completeness of the CPS and was not convinced all concerns had been addressed. The FPKIPA agreed that the CPWG should continue to address the issue and report to the FPKIPA.

The FPKIPA agreed that the CPWG should continue to address the issue and report to the FPKIPA.

Agenda Item 8

FPKI Management Authority (FPKI MA) Report—Wendy Brown

a. SIA Extension Update
After the report from the TWG at the last PA meeting regarding the Microsoft decision not to include the Common Policy Root certificate containing the SIA extension in their trusted Root Store, it was requested that the MA poll the FPKI Community and PKI vendors whether any applications would not be able to perform certificate validation if the SIA extension was not required in CA certificates.

Ms. Brown said the FPKI MA had polled the technical POCs of the cross-certified entities, as well as the SSPs and PKI vendors. While we have not yet received responses from all parties so far, nobody has a requirement for the SIA extension and some would prefer it to go away.

b. Sunset X.500 Chaining Update
This poll of cross-certified entities found that one member agency relies on X.500 chaining to do path discovery and validation, most others have responded that they only support X.500 chaining because it was a requirement of the Federal Bridge.

c. HTTP vs. LDAP
The FPKI MA found that SAFE has a requirement for using LDAP in the CDP extension, but not for AIA and SIAs. Most other responders so far have not felt LDAP URLs should remain mandatory but LDAP should continue to be supported.

d. SHA-256 Requirement
The Common Policy CP requires that CRLs and certificates issued starting in 2011 have to be signed using SHA-256 or SHA-384. The existing Common Policy CA does not have this capability. The FPKI MA is in talks with Microsoft about upgrading the CA. One SSP has already asked if they could send a PKCS-10 signed with SHA 256. The MA will continue to meet with the CA vendors to ascertain if and when they can meet this requirement..

e. IPSecv6
The Federal Government is moving toward implementing IPSecv6. The MA is looking into IPSecv6 to determine if its security features can be leveraged in the redesign effort.

Agenda Item 9

***Update on SSP and* SSPWG Activities—Judith Spencer**

Ms. Spencer said that due to current FISMA guidance, the GSA SAISO thinks that the trusted roles of all SSPs should undergo NAC-I background checks. The SAISO interpretation is that SSPs are running IT systems on behalf of the federal government, so they must satisfy expanded security requirements. The issue is open to interpretation and has operational and cost implications to the SSPs. Because GSA does Certification and Accreditations on the SSPs, the GSA SAISO believes the NAC-I is required under an 800-53 control. Ms. Spencer maintains that SSPs are providing “services,” not running “systems,” and, therefore not subject to expanded government security controls. Another SAISO concern is that PII may be held by the providers, but the SSPs do not hold PII; and the RA function, which does, is done locally by the Agencies.

The interpretation selected is an agency decision and many agencies are facing the same problem, she said. This is a big issue for Treasury, for example, because they outsource practically everything. There was general agreement that SSP functions should be interpreted as services, not operations of IT systems on behalf of the government.

The FPKIPA also discussed whether SSP staff in trusted roles should have security clearances, but did not come to any conclusions. Judy Spencer asked the members if they could check with the appropriate offices in their agencies on this issue.

Agenda Item 10

Final Meeting Items

1. Other Topics
    a. Dr. Alterman said the National Notary Association is going digital with Medium Hardware certs from SAFE Bio-Pharma via SAIC.
    b. Ms. Spencer said she and John Hannan met two weeks ago with Adobe (John Landwehr) to discuss getting the Common Root certificate onto the Adobe Trust List so that citizens can verify PIV credentials used to sign pdf-formatted documents. She is providing a PIV credential with digital signatures to Adobe for testing. The first step is to get Common included in the Adobe trust list. It is possible the legacy agencies will have to make their own arrangements with Adobe.

2. Proposed Agenda Items for the next FPKIPA meeting, 12 August 2008. Results of three e-votes:
    a. Discuss/Vote to accept FBCA CP Change Proposal: 2008-02 (archiving)
    b. Discuss/Vote to accept FBCA CP Change Proposal: 2008-03 (Auditor Independence)
    c. Discuss/Vote to accept Common Policy Change Proposal: 2008-01A (Auditor Independence)

3. FPKIPA Action Item review (please scrub this list BEFORE the 12 August 2008 FPKIPA meeting)

Agenda Item 11

Adjourn Meeting

Dr. Alterman adjourned the FPKIPA meeting at 11:50 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
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

No.	Action Statement	POC	Start Date	Target Date	Status
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