Minutes of the 10 June 2008 Meeting

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

A. AGENDA

a. Welcome / Introductions
b. Discussion / Vote on 13 May 2008 FPKIPA Minutes
c. FPKI Certificate Policy Working Group (CPWG) Report
    i. Discuss CPWG Recommendation to accept Wells Fargo Audit Letter and Management Assertion
    ii. Discuss/Vote on cross-certification of Wells Fargo (new CA) at Medium, Medium Hardware, Medium CBP and Medium Hardware CBP
    iii. Discuss CPWG Recommendation regarding SAFE Bio-Pharma CP v2.2—E-Auth Level 3 Level of Assurance
    iv. DoD Change Proposal (CA entity life)
    v. USPS Mapping Efforts
d. FPKI Management Authority (FPKI MA) Report
    i. Certificate Directory Status
    ii. Cross-Certification Status
    iii. Interoperability Testing
    iv. Contingency Plan Testing
    v. FPKIA Re-design
    vi. New FPKI MA Operational Procedure on Emergency Removals
    vii. Report on the FBCA TWG meeting, May 30, 2008: SIA Extension in the Common Policy Root certificate and ramifications of Microsoft declining to include it in their trusted Root Store
e. *Update on SSP and* SSPWG Activities
    i. VeriSign Business Application
    ii. Verizon Business Application
    iii. IdenTrust C&A
f. Final Meeting Items
    i. FPKIPA Chair's Report on FAA Meeting
    ii. X.509 Profile Question
    iii. Proposed Agenda Items for the next FPKIPA meeting, 8 July 2008
        1. Results of the E-vote on Wells Fargo cross-certification at Medium, Medium CBP, Medium Hardware and Medium Hardware CBP
        2. Briefing on the use of HTTP instead of LDAP

3. Vote on the Verizon Business Application for Cross-Certification with the FBCA

iv. FPKIPA Action Item review (please scrub this list BEFORE the 8 July 2008 FPKIPA meeting)

g. 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	Teleconference
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)	Jewell, Chris	Teleconference
GPO	Absent	
GSA	Temoshok, David	
NASA -Alternate	Levine, Susan	Teleconference
Nuclear Regulatory Commission- NRC	Sulser, David	
SSA	Absent	
USPS	Stepongzi, Mark	
USPTO	Absent	

OBSERVERS

Organization	Name	Telephone
FPKI Management Authority (MA)/GSA	Jenkins, Cheryl	Teleconference
eValid8	Dilley, Brian	
NOAA (Contractor, General Dynamics)	Wright, Bill	
IdenTrust	Schambach, Marco	Teleconference
Department of State/ Co-chair, CPWG (Contractor, ManTech)	Froehlich, Charles	
Wells Fargo	Gross, Jim	Teleconference
GSA (Legal Counsel)	Cornell, John	Teleconference
FPKI/FICC Support (Contractor--FC Business Systems LLC)	Petrick, Brant	

Organization	Name	Telephone
FPKIPA Secretariat (Contractor -- Protiviti Government Services)	Fincher, Judy	
SAFE Bio-Pharma	Cullen, Cindy	Teleconference
SAFE Bio-Pharma	Zagar, Terry	Teleconference
SAFE Bio-Pharma	Schoonmaker, Jon	
FPKI Management Authority (MA) Technical Lead (Contractor—Protiviti Government Services)	Brown, Wendy	
FPKI PA Support/Co-Chair CPWG (Contractor, Protiviti Government Services)	McBride, Terry	Teleconference
MIT Lincoln Laboratory IT Security, ICS	Malabon, Mikiala	Teleconference
FPKIPA Support (Contractor, Protiviti Government Services)	King, Matt	Teleconference

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 13 May 2008 FPKIPA Minutes—Judy Fincher

Ms. Fincher said she incorporated all the comments received on the 13 May 2008 FPKIPA minutes. She distributed the redline version along with the agenda and meeting notice five business days prior to the 10 June 2008 meeting. Wendy Brown made one verbal change at the meeting and Ms. Fincher accepted it.

The FPKIPA voted by 10/15, or 67%, to approve the minutes, as amended, where a 50% majority was required.

Approval vote for 13 May 2008 FPKIPA Minutes – red line version, as amended			
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	√		
Department of Justice	√		
Department of State	√		
Department of the Treasury	Absent		
Drug Enforcement Administration (DEA CSOS)	√		
GPO	Absent		
GSA	√		
NASA	√		
Nuclear Regulatory Commission	√		
SSA	Absent		
USPS	√		
USPTO	Absent		

Agenda Item 3

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

a. Discuss CPWG Recommendation to accept Wells Fargo Audit Letter and Management Assertion

The FPKIPA held a lengthy and sometimes contentious discussion as to the adequacy of the Wells Fargo audit. A single variance was identified and an approach outlined to resolve the issue.

Dr. Alterman: We perform audits on the previous version. In the case of Wels Fargo, the audit was performed on the then current CP Version 11—although the next audit cycle will be against Version 12, the version to be cross-certified.

Debbie Mitchell (DoD): She disagreed that the only issue with the Wells Fargo audit concerned an archiving issue that had been resolved. She raised the issue that DoD concerns with the Wells Fargo audit had been documented and were discussed at the 5 June 2008 CPWG meeting. The end-result of the discussion at the CPWG meeting was that John Cornell was drafting a letter for Dr. Alterman's signature to send to Wells Fargo to obtain some answers to issues that were raised.

David Temoshok summarized the above discussion, for the record:

1. The only policy mapping variance of the WF CP to CPS and compliance audit was the issue of 10 1/2 years record archiving.
2. After discussion it was agreed that FPKIPA can accept corrective action to audit findings.
3. WF has expressed that they will comply with CP requirement for 10 1/2 years record archiving.
4. As CPWG has gone on the record that they do not recommend acceptance of the WF Compliance Audit and Management Assertion at this time, the CPWG

(John Cornell) had drafted a letter for FPKIPA Chair to send to WF to list deficiencies to be addressed.
5. The FPKIPA should defer the vote until Wells Fargo's response to the FPKIPA Chair's letter is received, reviewed, accepted.

ACTION: The FPKIPA will conduct an e-vote on the cross-certification of the new Wells Fargo CA at Medium, Medium Hardware, Medium CBP and Medium Hardware CBP before the July 8, 2008 FPKIPA meeting. This e-vote should not occur until Wells Fargo's response to the FPKIPA Chair's letter is "received, reviewed, and accepted."

b. Discuss CPWG Recommendation regarding SAFE Bio-Pharma CP v2.2—E-Auth Level 3 Level of Assurance

Terry McBride led the discussion of this agenda item. He said that SAFE had modified its Basic and Medium CBP CPs to accommodate a roaming solution, using a FIPS-2 validated, USB token.

Ms. Spencer sent out the CPWG recommendation prior to the FPKIPA meeting, after discussions between the CPWG (Judy Spencer, Jon Schoonmaker and Terry McBride) with NIST (Bill Burr and Donna Dodson). NIST reviewed and validated the multi-factor cryptographic token and agreed that it meets Level 3 Authentication.

The CPWG recommendation stated that SAFE Bio-Pharma Change Proposal submitted to the CPWG for review meets the requirements for E-Auth Level 3, e.g., their CP is fine for continued mapping against Basic and Medium CBP.

c. DoD Change Proposal (CA entity life)
Mr. Froehlich said he was still waiting for edits by DoD to their Change Proposal. The CPWG will discuss the revised Change Proposal at its 17 June 2008 meeting.

d. USPS Mapping Efforts
The CPWG successfully mapped the General Matrix (3647-format) at its last meeting, although there are a few outstanding issues that USPS needs to clarify. The CPWG will begin mapping the USPS Medium Hardware (3647-format) matrix at its 17 June 2008 meeting.

Agenda Item 4

FPKI Management Authority (FPKI MA) Report—Cheryl Jenkins, Terry McBride, Wendy Brown

a. Certificate Directory Status

- The FPKI MA scheduled their Contingency Plan test for 5/19-6/2/2008, but it ended early--on 5/26.
- The FPKI MA lost power at the Primary Site on 6/4/2008 and had to roll to the Backup Site that evening. The MA moved back to the Primary Site on 6/9/2008 after power was restored on Friday p.m., 6/6/2008. On both occasions, the MA was successful in moving operations to the Backup Site. Some customers had trouble because they had an IP address in their certificate--rather than the DNS.
- During May 2008, both DHS and GPO experienced brief outages of their directories.

b. Cross-Certification Status

The FPKI MA issued one (1) cross-certificate from the Bridge CA to DHS to hold them over until they move to their SSP. We have received word that they have now moved to their SSP. As of 6/9/2008, DHS will discontinue operation of the CA cross-certified with the FBCA. Consequently, the interim cert will be revoked.

c. Interoperability Testing

The FPKI MA is still waiting to perform interoperability testing at C4 with University of Texas.

d. Contingency Plan Testing

The FPKI MA did the contingency test plan in May and used the plan when the primary site lost power.

e. New FPKI MA Operational Procedure on Emergency Removals

Ms. Jenkins announced a new, formalized procedure for emergency removals. At times, we will have to remove you immediately, without advance notification, because you are affecting an application. The MA, acting on its own authority, will remove you from the repository immediately if you are impacting the infrastructure.

In non-emergency situations, we will continue to color code the issues in the Statistical Report and give you a certain number of days to fix it, depending on the severity of the issue.

David Temoshok advocated formalizing this procedure in the standing FPKIPA documentation, moving forward.

Dr. Alterman said that an “emergency pull” is part of our operations, even though it is not currently included in the list of things we vote on—as per the Charter. An emergency pull is different from a revocation, which is covered already.

Mr. Temoshok said that a number of FPKIPA operational practices needs to be added to the By-Laws in the following areas:

a) Key recovery
b) Emergency removal
c) Encryption certificates
d) Audits

f. Report on the FBCA TWG meeting, May 30, 2008: SIA Extension in the Common Policy Root certificate and ramifications of Microsoft declining to include it in their trusted Root Store—Terry McBride

Mr. McBride gave a recap of the May 30, 2008 FBCA TWG meeting and said the major problem was with the Microsoft SIA design. Microsoft decided to pre-populate and pre-discover certification paths that use the SIA extension. This creates an on-going performance issue. Every time a cert fails, Microsoft tries that URL again and then re-runs the results every eight days.

Mr. McBride said the FPKI MA solution is to change policy, so that the Common Policy root would NOT contain the SIA. He said he would like to provide this solution to Microsoft.

Microsoft, in the meantime, has identified a "hot fix." Details will be ready in the late summer to early autumn timeframe. It has agreed not to chase SIA's recursively by default. For the medium to long-term, Microsoft will not accept any certificate with the SIA extension.

To assess the impact of these proposals on the FPKI community, the FPKI MA will contact the technical POCs of all cross-certified entities, as well as the SSPs. There was consensus that NIST should address the issue and provide guidance.

Agenda Item 5

Update on SSP and SSPWG Activities—Brant Petrick

a. VeriSign Business Application

We are waiting on various policy documents (e.g., CP) from VeriSign.

b. Verizon Business Application
We have received an Application from Verizon Business for cross-certification of the Cybertrust Commercial PKI with the Federal Bridge and it will need to be voted-on at the next FPKIPA meeting.

.

c. IdenTrust C&A

Mr. Petrick said an email has been sent to IdenTrust, requesting them to address certain audit-related items.

Agenda Item 6

Final Meeting Items

a. FPKIPA Chair's Report on FAA Meeting
   On 22 May 2008, Dr. Alterman attended an FAA meeting with representatives of EADS, AirBus, Northrop Grumman, Lockheed Martin, et al. FAA is considering using VeriSign SSP. There are plans to expand PKI for documents that the airlines submit to the FAA, he said. There is a lot of ferment to use PKI to enable business processes, apart from the HSPD-12 related initiatives.
b. Proposed Agenda Items for the next FPKIPA meeting, 8 July 2008
   1) Results of the E-vote on Wells Fargo cross-certification at Medium, Medium CBP, Medium Hardware and Medium Hardware CBP
   2) Briefing on the use of HTTP instead of LDAP
   3) Vote on the Verizon Business application for cross certification with the FBCA
c. FPKIPA Action Item review (please scrub this list BEFORE the 8 July 2008 FPKIPA meeting)

Agenda Item 10

Adjourn Meeting

Dr. Alterman adjourned the meeting at 11:28 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

No.	Action Statement	POC	Start Date	Target Date	Status
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
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
332	Debbie Mitchell will copy the FPKIPA and CPWG ListServs on the comments they provided to NIST on NIST SP 800-63-1.	Debbie Mitchell	8 April 2008	11 April 2008	Open
333	Dr. Alterman will send out an e-mail with an attachment explaining the process and procedures followed by the FPKIPA to maintain the Provisional Basic Cross-Certification with Wells Fargo through the end of March 2008.	Dr. Peter Alterman	8 April 2008	11 April 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
369	A sub-committee of the CPWG will hold a teleconference with Wells Fargo before the May 20 CPWG meeting to resolve the CPS issue.	CPWG Sub-Ctee, Wells Fargo	13 May 2008	19 May 2008	OPen
370	The FPKIPA will conduct an e-vote on the cross-certification of the new Wells Fargo CA at Medium, Medium Hardware, Medium CBP and Medium Hardware CBP before the July 8, 2008 FPKIPA meeting. This e-vote should not occur until Wells Fargo's response to the FPKIPA Chair's letter is "received, reviewed, and accepted."	CPWG, Dr. Alterman, Judith Fincher	10 June 2008	8 July 2008	Open