Minutes of the 10 March 2009 Meeting

USPS, 475 L'Enfant Plaza, SW, Washington, DC
Conference Room 2P316

A. AGENDA

1. Welcome / Introductions
2. Discuss/Vote on 10 February 2009 FPKIPA Minutes
3. Status Report on the Realized Value of PKI
4. Report on Compliance with the 3647 RFC CP/CPS Format
5. Update on the Antecedent Task Force Activities
6. Formal Acceptance of the Wells Fargo Decommissioning
7. FPKI Certificate Policy Working Group (CPWG) Report
    a. Discuss/Vote to Cross-Certify Verizon Business Systems at Basic, Medium, Medium CBP, Medium Hardware and Medium Hardware CBP
    b. Discuss Cross-Certifying SAFE Bio-Pharma at Basic
8. FPKI Management Authority (FPKI MA) Report
9. Update on ISIMC/ICAMSC
10. Other Agenda Items
    a. Updating the Charter and By-Laws
    b. Meeting Location for July 14, 2009
    c. Access to the DoD Path Validation Tool
    d. DoD Identity Management Conference

11. 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. Additionally, another member joined late, bringing the ratio to 13/15 (86.7%).

Organization	Name	Telephone
Department of Commerce (NIST)	ABSENT	
Department of Defense	Mitchell, Debbie	
Department of Health & Human	Slusher, Toby	Teleconference

Organization	Name	Telephone
Services		
Department of Homeland Security	Miller, Shawneque (Tanyette)	
Department of Justice	Morrison, Scott	
Department of State	McCloy, Mark	
Department of Treasury	Schminky, Jim	
Drug Enforcement Administration (DEA CSOS)	ABSENT	
GPO	Hannan, John	
GSA	Spencer, Judith	
NASA	Levine, Susan	Teleconference
Nuclear Regulatory Commission- NRC	Sulser, David	
SSA	Mitchell, Eric	
USPS	Stepongzi, Mark	
USPTO	Lindsey, Dan	Teleconference

OBSERVERS

Organization	Name	Telephone
FPKIPA Support/Secretariat (Contractor, Protiviti Government Services	Fincher, Judy	
IdenTrust	Schambach, Marco	Teleconference
FPKI/ICAMSC Support (Contractor, Unisys	Petrick, Brant	
Department of State/ Co-chair, CPWG (Contractor, ManTech)	Froehlich, Charles	
EOP	Smith, Winsfield	Teleconference
NIST	Cooper, David	Teleconference
Wells Fargo	Schwartz, Ruven	Teleconference
SSA	Jackmon, Kenya	Teleconference
PM/FPKI MA/GSA	Jenkins, Cheryl	
eValid8	Dilley, Brian	
FPKI MA Technical Liaison (Contractor, Protiviti Government Services)	Brown, Wendy	
FPKIPA Support, Co-Chair CPWG (Contractor, Protiviti Government Services)	McBride, Terry	
GSA	Murdock, Rachael	
DOE	Lonnerdal, Nils "Daniel"	
DOE	Varghese, Jebby	
Cipher Solutions, Inc.	Ahuja, Vijay	
SAFE Bio-Pharma (Chair, Antecedent Task Force)	Schoonmaker, Jon	Teleconference

C.   MEETING ACTIVITY

Agenda Item 1

Welcome / Introductions—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. Judith Spencer, Interim Chair, called the meeting to order at 9:40 a.m. and conducted introductions of those present in person and via teleconference. We wish to thank Mark Stepongzi of the USPS for hosting the meeting.

Agenda Item 2

Discuss/Vote on 10 February 2009 FPKIPA Minutes— Judy Fincher

The FPKIPA approved the redline February 10, 2009 FPKIPA minutes, unanimously (13/13) or 100% where a 50% majority vote was required. Commerce and DEA CSOS were absent for this vote.

Approval vote for 10 February 2009 FPKIPA Minutes – red line version			
	Vote (Motion- NRC, 2nd- Treasury)		
	Yes	**No**	**Abstain**
Department of Commerce	ABSENT		
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)	ABSENT		
GPO	√		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC)	√		
SSA	√		
USPS	√		
USPTO	√		

Agenda Item 3

Status Report on the Realized Value of PKI—Judith Spencer
Ms. Spencer reported on the response of the Cross-Certified entities to her request for documentation on their experience with PKI, i.e., the "Realized Value of PKI." So far, only four entities have responded: DoS, GPO, and the Four Bridges Forum (4BF), incorporating responses from SAFE and CertiPath. DoD and NASA are planning to submit their responses by Friday of this week. Ms. Spencer appealed to other Federal agencies to document how they are faring with their own PKIs and send these reports to her ASAP.

The contractor, Protiviti Government Services (PGS), will compile this information and draft the report. The report will provide a 1) general overview of FPKI since the publication in June 2000 of "The Evolving Federal Public Key Infrastructure;" 2) general information on the value of PKI, 3) and case studies of agency and entity experiences with PKI. The internal deadline for this [draft] report is March 27, 2009. This will entail interviews with Dr. Peter Alterman, Judith Spencer, Chris Louden and other FPKI experts.

Agenda Item 4

Report on Compliance with the 3647 RFC CP/CPS Format—Judith Spencer

Ms. Spencer said that two years ago the FPKIPA issued a policy memo requesting that all cross-certified entities become compliant with RFC 3647 CP/CPS format. Most have made that change or have come in using that format, e.g., VeriSign, Verizon. Those who have not yet complied include Justice and USPTO. Justice has re-written their CP/CPS to comply, but the Justice PMA has not yet signed off on it. Dan Lindsey of USPTO, who is new to the FPKIPA, is checking on the status of that activity. GPO is actively working on their documentation and expect it to be completed within a month or so. DoE will need to be compliant with RFC 3647 if they reapply to have their CA cross-certified with the FBCA.

Agenda Item 5

Update on Antecedent Task Force Activities—Judith Spencer, Jon Schoonmaker (SAFE)

The Antecedent Task Force is working on a definition of In-Person Antecedent (IPA) that will support Medium Hardware. They have briefed the CPWG twice (February 5 and March 5) on the requirements and recommended policy. They meet on a regular basis (each Thursday) and expect to have a revised draft of the proposed In-Person Antecedent policy to Ms. Spencer by March 19. Once a definition is agreed, it will be published on the FPKIPA website and will be referenced in FBCA policy. NIST will be encouraged to accommodate this requirement in the revised NIST SP 800-63-1, Ms. Spencer said. The definition must include a pre-existing relationship with a Trusted Agent, she added, to meet Medium Hardware requirements.

Ms. Spencer said that NIST SP 800-63-1 currently limits IPA to the banking community. It is a disjointed, contradictory treatment of the topic, she said. She provided written comments to NIST on 800-63-1 and is in conversation with Tim Polk of NIST, one of the principal authors.

Debbie Mitchell, who submitted the Change Proposal that kicked off this activity, objected to the sequencing of events. It seems we will be out-of-synch if 800-63-1 is not changed. It would be better to wait until 800-63-1 is finalized and then revisit the Change Proposal, she said.

Meanwhile, the Change Proposal is tabled until we come up with a satisfactory IPA definition and model.

Ms. Spencer said that the Justice CEO (Van Hitch) wants to do IPA for remote [prison] personnel, using a PIV card. David Sulser reported that there have been lots of interest and requests at NRC in using IPA.

Agenda Item 6

Formal Acceptance of the Wells Fargo Decommissioning—Judith Spencer

close notice 12 2008.doc

Ms. Spencer said Wells Fargo has notified the FPKIPA in writing   that it is discontinuing issuance of new and renewal of existing WellsSecure Federal Bridge certified digital certificates,. This document was distributed prior to the meeting to the FPKIPA listserv and a targeted e-mail went to the FPKIPA voting members. Wells Fargo will support already issued certificates until they expire on March 5, 2011 two years from the date of the final certificate issued by the WellsSecure service, according to Ruven Schwartz from Wells Fargo, who participated via teleconference. Initially, it was to end support on January 31, 2011, but Wells Fargo recently issued another cert (a special request).

The FPKIPA acknowledged receipt of this message, with regret.

Agenda Item 7

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

   a. Discuss/Vote on Cross-Certifying Verizon Business Systems at Basic, Medium, Medium CBP, Medium Hardware and Medium Hardware CBP

   The FPKIPA voted to cross-certify Verizon Business Systems at Basic, Medium, Medium CBP, Medium Hardware and Medium Hardware CBP at this meeting by a vote of 13/15 where a 75% majority vote of voting members was required. Ms. Spencer reminded the FPKIPA that the MOA has to be in place before we can execute the LOA. She and John Cornell will work with Verizon Business Systems on finalizing the MOA.

Vote to Cross-Certify Verizon Business Systems at Basic, Medium, Medium CBP, Medium Hardware and Medium Hardware CBP			
	Vote (Motion-Treasury, 2nd GPO)		
	Yes	No	Abstain
Department of Commerce	ABSENT		
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)	ABSENT		
GPO	√		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC)	√		
SSA	√		
USPS	√		
USPTO	√		

b. Discuss Cross-Certifying SAFE Bio-Pharma at Basic

Mr. Froehlich said the CPWG could not yet recommend that SAFE Bio-Pharma be mapped at Basic because they have yet to provide certain information.

Agenda Item 8

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

a) FPKI MA Report
Wendy Brown reported that the FPKIA directory has been stable this past month. One minor outage occurred in February due to hard drive problems with the web server, the MA hopes to remedy the hardware problems in March. The MA issued 3 cross certificates to VeriSign from the FBCA and are waiting for them to send back their cross certificates. The MA also reissued the ORC SSP 2 certificate from the Common Policy due to a problem with the encoding of the SKI (Subject Key ID).

IdenTrust wants to change directories (e.g., change their X.500 Directory to an LDAP only Directory), and is waiting for permission to start the interoperability testing. The FPKIPA agreed this was a non-contentious issue and that no vote was required and the MA was given approval to test the new IdenTrust directory. This means that IdenTrust will have to revise their MOA, e.g., include an addendum, and their CP, if it calls out X.500 as the directory.

b) FPKI Technical Advisory Group (TAG) Report

The FPKIPA previously had voted to make the SIA extension optional until 2010. Since NIST had not yet updated the profiles, Ms. Jenkins asked the TAG to review the SIA issue.

Here are the major findings of that report (due out on Friday, March 13, 2009)

1. The TAG recommends the FPKI not use the SIA extension. Currently, the problems caused by the extension significantly outweigh the benefits. The extension should be optional, but its use is discouraged.

2. Where the SIA is used, it must point to publicly accessible and highly available URIs containing accurate information. LDAP URIs cannot meet this test as outbound LDAP is blocked by some agency firewalls.

3. SIA strategies and guidance should be coordinated and shared with the 4BF.

4. Making the SIA optional may eliminate the possibility of automatically and deterministically discovering the full trust path of the Federal Government, which may be harmful. The TAG is investigating alternative methods to find the full trust path of the Federal Government that do not require the SIA.

In summary, Ms. Jenkins said, we want it to be "optional" in the profile and we discourage its use in certificates sent to/from the Bridge. It should not appear in any certificates issued to FBCA and Common. It should never be contained in cross certificates issued back to the Federal Bridge.

Ms. Spencer said she would send a request to NIST (David Cooper) to make that extension optional in all profiles where it is currently mandatory. Ms. Brown said three worksheets are affected.

Debbie Mitchell stated that the agencies need to assess the impact of making it optional. Would this require re-testing?

Dave Cooper asked if we had the same problem with the AIA extension. Ms. Brown said no. Although the use of LDAP URIs in AIA may be unreachable from agencies that block outbound LDAP, the processing of AIA is different then SIA. It is not generally used to pre-populate a cache. Instead it is used to build a finite path up from an end-entity certificate.

Ms. Spencer stated that for the moment, the SIA has far greater impact and the PA has already voted to make it optional. And, she said, we are limiting this profile update to the SIA extension.

Ms. Jenkins said we need a Change Proposal to force technical guidance and a Practice Note in the FBCA CP.

Agenda Item 9

Update on ISIMC/ICAMSC—Judith Spencer

a. Judy Spencer said that the ICAMSC met two weeks ago. The next meeting is March 24. If you do not know who your ICAMSC member is, send me an e-mail.
b. Ms. Spencer said that the ICAMSC is building the primary pieces of the Segment Architecture and drafting an implementation guide for IdM, both due out in June for use in preparing the 2011 Annual Budget Submission.
c. She reminded the FPKIPA membership that the e-Authentication Program office has been merged into the ICAMSC. The program office no longer exists, but the policy, M-04-04, does, she said.

    d. Ms. Spencer said that a Citizen Outreach focus Group will be interfacing with the American public. The new Federal CIO is big on Open ID, probably at Levels 1 & 2, she said. The GSA ICAM is looking forward to assisting. GSA is in the process of hiring Senior Policy Analysts to support this and other work.

Agenda Item 10

Other Agenda Items—Judith Spencer, Debbie Mitchell, Rachael Murdoch

    a. Updating the Charter and By-Laws: Rachael Murdock has received no comments from agencies on the Charter and By-Laws that she is editing. The comment period is open until March 20.
    b. Meeting Location for July 14, 2009: We have been bumped from our regular FPKIPA meeting room at USPS for July 14, 2009. Please let Judith Fincher know if you can host this meeting.
    c. Access to the DoD Path Validation Tool: Debbie Mitchell said the DoD Path Validation tool can be made available to its Federal partners. Send Ms. Mitchell an e-mail if you are interested in using the tool.
    d. DoD Identity Management Conference: Debbie Mitchell said the DoD Identity Management Conference is April 27 – May 1, 2009 in Miami, FL. Registration is now open at www.nsa.gov.

Agenda Item 11

Adjourn Meeting—Judith Spencer
Ms Spencer adjourned the meeting at 10:46 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
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
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
373	Deborah Gallagher will check with DHS to verify the FRAC requirement.	Deborah Gallagher	9 Sept. 2008	14 Oct. 2008	Open
375	The FPKIPA Chair will take the enduring proxy and meeting schedule issues under advisement and will notify non-attendees that they risk losing their voting privileges if they persist in unexplained absences and do not designate a proxy when they cannot attend.	Judith Spencer	14 October 2008	12 November 2008	Open
376	Debbie Mitchell will ask Camie Webster if the PKITHING tool and other tools used in the testing are available to the FPKIPA community	Debbie Mitchell	10 Feb. 2009	19 Feb. 2009	