



Minutes of the 14 April 2009 Meeting
National Institute of Standards and Technology (NIST)
Main Campus, W. Diamond Avenue, Gaithersburg, MD
Dining Room C
9:30 a.m. – 11:40 a.m.

A. AGENDA

1. Welcome / Introductions
2. Discuss/Vote on 10 March 2009 FPKIPA Minutes
3. FPKI PA Chair Appointment Process
4. Review Antecedent Issues Paper
5. Review/Vote on Entrust Application for Cross-Certification with the FBCA
6. FPKI Certificate Policy Working Group (CPWG) Report
 - a. CPWG Recommendation to accept Treasury's RFC 3647-formatted CP
 - b. Common CP Change Proposal: 2009-02: PKI-enabled authentication to be permitted as proof of identity in lieu of digital signatures
7. FPKI Management Authority (FPKI MA) Report
 - a. FPKI MA Report
 - b. SIA Extension
8. Update on ISIMC/ICAMSC
9. Other Agenda Items
 - a. Treasury compliance audit
 - b. Agency RPS
10. Adjourn Meeting

B. ATTENDANCE LIST

VOTING MEMBERS

The meeting began with a quorum of 11/15 (or 73.3%) where a two-thirds majority was required. Additionally, two additional members joined the meeting in process, bringing the ratio to 13/15 (86.7%).

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)	ABSENT	
Department of Defense	Mitchell, Debbie	Teleconference
Department of Health & Human Services	Slusher, Toby	Teleconference

Organization	Name	Telephone
Department of Homeland Security - proxy	Garcia, Gladys	Teleconference
Department of Justice	Morrison, Scott	Teleconference
Department of State	McCloy, Mark-joined after the vote on the minutes	Teleconference
Department of Treasury	Schminky, Jim	
Drug Enforcement Administration (DEA CSOS)	Jewell, Chris	Teleconference
GPO	Hannan, John	
GSA	Spencer, Judith	
NASA	Levine, Susan-joined after the vote on the minutes	Teleconference
Nuclear Regulatory Commission- NRC	Sulser, David	
SSA	ABSENT	
USPS –proxy	Weidenhamer, Charles	Teleconference
USPTO	Lindsey, Dan	

OBSERVERS

Organization	Name	Telephone
State of Illinois	Anderson, Mark	Teleconference
FPKIPA Support/Secretariat (Contractor, Protiviti Government Services)	Fincher, Judy	
IdenTrust	Schambach, Marco	Teleconference
IdenTrust	Corbo, Page	Teleconference
FPKI/ICAMSC Support (Contractor, Unisys)	Petrick, Brant	
Department of State/ Co-chair, CPWG (Contractor, ManTech)	Froehlich, Charles	
EOP	Smith, Winsfield	Teleconference
Wells Fargo	Schwartz, Ruven	Teleconference
PM/FPKI MA/GSA	Jenkins, Cheryl	
USPTO	Kless, Patricia	Teleconference
FPKI MA Technical Liaison (Contractor, Protiviti Government Services)	Brown, Wendy	
FPKI MA Support (Contractor, Protiviti Government Services)	Louden, Chris	
SAFE Bio-Pharma (Contractor, SAIC)	Danfield, Paul	
DHS PKI Operational Authority	Koren, Bill	Teleconference
Treasury	Robinson, Michael	
Cipher Solutions, Inc.	Ahuja, Vijay	Teleconference
SAFE Bio-Pharma (Chair, Antecedent Task Force)	Schoonmaker, Jon	
CertiPath	Howard, Steve	Teleconference
CertiPath (Boeing)	Knoll, Jacqueline	Teleconference
FPKIPA Support (Contractor, Protiviti Government Services)	Tevelow, Mickey	Teleconference

C. MEETING ACTIVITY

Agenda Item 1

Welcome / Introductions—Judith Spencer, Interim Chair

The FPKIPA met at the National Institute of Standards and Technology, W. Diamond Avenue, Main Campus, Dining Room C., Gaithersburg, MD Judith Spencer, Interim Chair, called the meeting to order at 9:35 a.m. and conducted introductions of those present in person and via teleconference. We wish to thank Judith Spencer of GSA and Sara Caswell of NIST for hosting the meeting.

Agenda Item 2

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

The FPKIPA approved the redline March 10, 2009 FPKIPA minutes, unanimously (11/11) or 100% where a 50% majority vote was required. Commerce, DoS, NASA, and SSA were absent for this vote.

Approval vote for 10 March 2009 FPKIPA Minutes – red line version			
	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	ABSENT for this vote		
Department of the Treasury	√		
Drug Enforcement Administration (DEA CSOS)	√		
GPO	√		
GSA	√		
NASA	ABSENT for this vote		
Nuclear Regulatory Commission (NRC)	√		
SSA	ABSENT		
USPS	√		
USPTO	√		

Agenda Item 3

FPKI PA Chair Appointment Process—Judith Spencer

Ms. Spencer gave a history of the FPKIPA chair's requirements. The first FPKIPA Chair, Michelle Moldenhauer (Treasury), was appointed and served four years (two terms). We instituted the voting process in 2004, she said, and Dr. Peter Alterman was elected. He served two terms. He resigned in August 2008 to become Deputy Associate Administrator of Technology Strategy at GSA, and Judith Spencer has served as interim chair since that time.

In the early years of the FPKIPA, the chair was expected to make a 40% commitment. It has evolved into being a nearly full time job. It also required that the chair 1) participate in the CPWG, 2) and have the backing of his/her senior management for up to \$150,000 per year in salary and travel that is not paid for by the FPKIPA.

She said she believed the FPKIPA would be better served to have a GSA-appointed and financially backed chair. She plans to submit a proposal to that effect at the next meeting of the FPKIPA on behalf of her organization, the Office of Governmentwide Policy (OGP).

Jim Schminky said he felt the work of the Chair may again be closer to 40% because the role of the FPKIPA is somewhat diminished with the new reporting arrangement, e.g., to the CIO Council through the ISIMC through the ICAMSC. Ms. Spencer objected, saying she would continue to provide guidance and oversight to the new chair (whether elected or appointed), but would not micro manage. She felt strongly that a full-time commitment was needed to chair the FPKIPA. The role also entails speaking at conferences and considerable travel. She also wanted contract support to stay in GSA OGP, regardless of who becomes chair, though it might become murky if GSA had to pay for travel for another agency.

She suggested that the FPKIPA consider appointing a full-time chair and that she and Mr. Schminky submit proposals to the FPKIPA at the May meeting.

Everyone agreed that PKI is changing due to its central role in HSPD-12 implementations, i.e., the integration of PACS/LACS. The "Troubled Assets Relief Program" (**TARP**) {Public Law 110-343, 122 STAT. 3765, DOCID: f:publ343.110} has also raised PKI's visibility. Charles Froehlich said that NSS PKI CP (the classified PKI) says that classified CNSS systems will be required to use PKI through the NSS PKI infrastructure. Other NSS systems not processing at the classified level will get support from FPKI.

Ms. Spencer said the E-Gov act of 2002 is coming up for renewal and that she wants to start grooming her GSA/OGP replacement now, so that he/she would be ready in time. Ms. Spencer also plans to retire in 22 months, she said.

Agenda Item 4

Review Antecedent Issues Paper—Jon Schoonmaker, Paul Danfried

Jon Schoonmaker of SAFE Bio-Pharma introduced members of his team from the SAFE and CertiPath bridge communities. The team has been working on an In-Person Antecedent (IPA) policy since January 8, when the DoD submitted a Change Proposal to remove the IPA from the Medium Hardware policy. That Change Proposal has been tabled while the IPA team prepared use cases and supporting policy language.

At the April 14 meeting, Mr. Schoonmaker presented two use case scenarios: 1) Enterprise Use Case, 2) the Third Party Antecedent Use Case. The first use case includes a pre-existing relationship with a Trusted Agent, which is a Medium Hardware requirement. In the second use case, the trust relationship between the trusted agent and the applicant is derived from an "authoritative source and its verification of the in-person event."

The FPKIPA did not debate the merits of the two scenarios. The CPWG will review the revised Policy, Use Cases, and Change Proposal at their April 21 and May 7 meetings. After CPWG

review, the FPKIPA will again entertain the IPA draft policy, use cases and revised change proposal.

Ms.Spencer also noted that she is meeting with Bill Burr of NIST this week on proposed changes to IPA language in NIST SP 800-63, which is currently being edited.

Paul Danfried (SAIC/SAFE) noted that this process (Use Case 2) works about 85% of the time. Only in about 15% of the cases is it necessary to fall back to manual processes. He said that the cost of cracking a manual process, e.g., obtaining a false driver’s license, passport, utility bill receipts, etc., costs about \$15k; whereas, the cost of an automated crack is ~ \$150k. This scenario, he said, significantly raises the bar.

Agenda Item 5

Review/Vote on Entrust Application for Cross-Certification with the FBCA—Judith Spencer

Ms. Spencer said Entrust is following in the footsteps of VeriSign and Verizon Business Systems in seeking to cross-certify its non-Federal SSP “clone” PKI. Entrust is asking to be cross certified at Rudimentary, Basic, Medium, Medium Hardware, Medium CBP and Medium Hardware CBP.

The FPKIPA voted to approve the Entrust application to cross-certify with the FBCA by a vote of 13/15 (86.7%) where a 75% majority vote of voting members was required.

Vote to Approve Entrust Application for Cross-Certification with the FBCA			
	Vote (Motion-Treasury , 2nd USPTO		
	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)	√		
GPO	√		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC)	√		
SSA	ABSENT		
USPS	√		
USPTO	√		

Agenda Item 6

FPKI Certificate Policy Working Group (CPWG) Report—Mickey Tevelow (acting)

- a. CPWG recommendation to accept Treasury’s RFC 3647-formatted CP

Mickey Tevelow said Treasury is now in full compliance with the RFC 3647 format requirement for its CP. The FPKIPA accepted the CPWG's recommendation. No vote was required.

- b. Common CP Change Proposal: 2009-02 (PKI-enabled authentication to be permitted as proof of identity in lieu of digital signatures)

Mr. Tevelow said this Change Proposal affects Federal contractors only and allows the agency to accept PIV cards (PIV Auth cert) instead of digital signatures or in-person requests, for the purpose of authenticating the Federal sponsor. For example, if I (Federal government employee) authenticate to the system using my PIV credential (PIV Auth cert), that should suffice instead of digitally signing the record. Digitally signing is redundant. The only people who can sponsor in Common are Federal government employees.

The FPKIPA voted to accept this change proposal by a vote of 13/15 (86.7%) where a 75% majority vote of voting members was required.

Vote to approve Common CP Change Proposal: 2009-02 (PKI-enabled authentication to be permitted as proof of identity in lieu of digital signatures)			
	Vote (Motion-USPTO , 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)	√		
GPO	√		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC)	√		
SSA	ABSENT		
USPS	√		
USPTO	√		

Agenda Item 7

FPKI Management Authority (FPKI MA) Report—Cheryl Jenkins, Chris Loudon

- a) FPKI MA Report

Ms. Jenkins said that there were no operational issues. The core releases for the re-design should be completed by the end of calendar year 2009. She said the FPKIPA had already voted (twice) to make the SIA extension optional: once by e-vote and the other time (November 08).

- b) SIA Extension

Chris Loudon reported that the TAG had issued a Change Proposal – now in report format—and that it is at NIST for review by Dave Cooper.

The issue is one of NIST standards versus practical implementation and operational perspectives, Mr. Loudon said. There is a problem if you use the SIA extension in Microsoft. SIA should be optional, deprecated, and removed from current certs in use, he said. In particular, the SIA extension should be removed from critical cross-certs between the FBCA and Common. At issue is only the CA repository field in SIA. The time stamping part of the SIA extension is Okay, he said. At issue is the required LDAP URI in SIA. A lot of agencies block outgoing LDAP, he said.

If SIA goes away, we will still need the AIA extension according to Mr. Loudon.

Agenda Item 8

Update on ISIMC/ICAMSC—Judith Spencer

Ms. Spencer reported that the “PIV Interoperability for Non-Federal Issuers” guidance was approved by the ISIMC and that Paul Fitzgerald of the ISIMC is doing the cover letter.

Ms. Spencer said she is meeting with the Open ID Foundation at the RSA Conference next week. Under consideration is the possible use of level 1 for Feds to citizen outreach, but also possibly, at levels 2 and 3 (M-04-04). We would need to overlay it to get to Levels 2 and 3, she said. Entrust, VeriSign and Verizon Business are also doing things with Open ID and we plan to have them in to talk, she said.

Agenda Item 9

Other Agenda Items—Jim Schminky, Judith Spencer

- a) Treasury compliance audit
Jim Schminky said the Treasury SSP Audit letter will be done this week.
- b) Agency RPS:
The RPS is done at the customer site and the Federal Government is responsible for auditing it, Ms. Spencer said. She has talked with some of the SSPs (Entrust, VeriSign, and Verizon Business) and that they help the customer write the RPS. They require their Federal customers to say they are compliant, perhaps as part of their C&A.

Agenda Item 10

Adjourn Meeting—Judith Spencer

Ms Spencer adjourned the meeting at 11:40 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	