



Minutes of the 12 January 2010 Meeting
USPS, 475 L'Enfant Plaza, SW, Washington, DC.
CR 2P316 (inside CR 2P310)
9:45 a.m. – 11:50 a.m.

A. AGENDA

- 1. Welcome / Introductions**
- 2. Discuss/Vote on 10 November 2009 FPKIPA Minutes**
- 3. Discuss/Vote on 8 December 2009 FPKIPA Minutes**
- 4. Discuss Asserting COMMON Policy OIDs outside of PIVauth and cardAuth for signature or encryption**
- 5. Briefing on the Proposed Triennial Compliance Audit Requirements**
- 6. FPKI Certificate Policy Working Group (CPWG) Report**
 - *Discuss / Vote: FCPF CP Change Proposal on Cryptographic Key Length*
 - *Discuss / Vote: FBCA CP Change Proposal—CA Remote Administration*
 - *Discuss / Vote: FCPF CP Change Proposal—CA Remote Administration*
- 7. FPKI Management Authority (FPKI MA) Report**
- 8. Other Agenda Items**
- 9. Adjourn Meeting**

B. ATTENDANCE LIST

VOTING MEMBERS

The meeting began with a quorum of 12/14 (or 85.7%) where a two-thirds majority was required. Two other voting members joined after the quorum was established, thus bringing the total to 100%.

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 were 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 Defense	Mitchell, Debbie	
Department of Health & Human Services	Slusher, Toby	Teleconference
Department of Homeland Security	Miller, Tanyette	Teleconference
Department of Justice	Morrison, Scott	

Organization	Name	Telephone
Department of State	McCloy, Mark	
Department of Treasury	Schminky, Jim	
Drug Enforcement Administration (DEA CSOS)	Jewell, Chris	Teleconference
GPO	Hannan, John	
GSA	Spencer, Judith	
NASA	Levine, Susan	Teleconference
Nuclear Regulatory Commission- NRC	Sulser, David	
SSA	Mitchell, Eric	Teleconference
USPS	Stepongzi, Mark	
USPTO	Lindsey, Dan	Teleconference

OBSERVERS

Organization	Name	Telephone
Entrust (vendor)	Moore, Gary	
FPKI MA/PM	Jenkins, Cheryl	Teleconference
State of Illinois	Anderson, Mark	Teleconference
IdenTrust	Schambach, Marco	Teleconference
KPMG	Faut, Nathan	
GSA Support (Contractor, Unisys)	Petrick, Brant	
DOE	Lonnerdal, Nils	
GSA Support (Consultant, RJ Schlecht Consulting)	Schlecht, R.J.	
FPKIPA (Contractor, PGS)	Fincher, Judy	
FPKI PA (Contractor, PGS)	McBride, Terry	
FPKI MA Technical Liaison (Contractor, Protiviti Government Services)	Brown, Wendy	
DOE (Contractor, M Squared Strategies, Inc.)	Olson, Evan	
Cipher Solutions (vendor)	Ahuja, Vijay	
DHS (Contractor, Protegus)	Shomo, Larry	Teleconference
SSA (Contractor, Jacob & Sundstrom)	Jackmon, Kenya	Teleconference

C. MEETING ACTIVITY

Agenda Item 1

Welcome / Introductions—Judith Spencer, Chair

The FPKIPA met at the USPS Headquarters, 475 L'Enfant Plaza, SW, Washington, DC, CR 2P316 (inside CR 2P310). Judith Spencer, Chair, called the meeting to order at 9:45 a.m. and conducted introductions of those present in person and via teleconference. We wish to thank Mark Stepongzi of USPS for hosting this meeting. The meeting started with a quorum (12/14) or 85.7% of voting members, and two members joined during the meeting.

Agenda Item 2

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

Ms. Fincher said all comments were incorporated and Ms. Spencer called for a vote to approve the minutes, as edited. The motion passed by 12/14 of 85.7% where a 50% majority vote was required. GPO and NRC had not yet joined the meeting.

Vote to approve 10 November 2009 FPKIPA Minutes			
	Vote (Motion- Treasury 2nd- USPS)		
	Yes	No	Abstain
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	ABSENT		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC)	ABSENT		
SSA	√		
USPS	√		
USPTO	√		

Agenda Item 3

Discuss/Vote on 8 December 2009 FPKIPA Minutes—Judy Fincher

Ms. Fincher said all comments were incorporated and Ms. Spencer called for a vote to approve the minutes, as edited. The motion passed by 12/14 of 85.7% where a 50% majority vote was required. GPO and NRC had not yet joined the meeting.

Vote to approve 8 December 2009 FPKIPA Minutes			
	Vote (Motion- DoS 2nd- Treasury)		
	Yes	No	Abstain
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	ABSENT		
GSA	√		
NASA	√		

Nuclear Regulatory Commission (NRC)	ABSENT
SSA	√
USPS	√
USPTO	√

Agenda Item 4

Discuss Asserting COMMON Policy OIDs outside of PIVauth and cardAuth for Signature or Encryption—Debbie Mitchell

Ms. Mitchell said DoD is considering asserting Common Policy OIDs in encryption and e-mail signing certificates, in order to be more interoperable with Federal partners. She wanted to know if other agencies were also considering doing this and whether there was a process in place.

Ms. Spencer said that DoD would have to subordinate under COMMON and that it would have far-reaching implications. This would change the way we are doing COMMON currently for SSPs, she said. You would have to be able to comply with FIPS 201, section 5.4.4.¹ To do more, we would have to accept you as subordinating to COMMON, she said.

Ms. Mitchell said that subordinating under COMMON was not acceptable to the DoD.

The stipulation would be that DoD runs their annual audit against COMMON, if they were to subordinate.

Ms. Mitchell asked if other agencies were considering this.

Jim Schminky (Treasury) said if path processing and validation are the issue he did not want to do “work-a-rounds,” and that the product vendors should fix these problems. Mr. Schminky said he wants to get Path Validation products on board and working. As we go forward and the use of PKI grows, maybe we can reach critical mass through PIV-I and solve these problems.

Mark McCloy (DoS) said he is trying to solve problems with their external partners directly, and not through the Federal Bridge.

Ms. Spencer said that the Logical Access Working Group met with Microsoft in November and that Microsoft has published documents concerning PIV enablement.

Larry Shomo (DHS) said it might be necessary for the legacies to have dual roots for the lower assurance levels. There is an explosion of PKI enabling going on at DHS. We need to pressure vendors to fix it; else, the Federal Government should not be buying their products.

¹ **FIPS 201, 5.4.4 Migration from Legacy PKIs**

Departments and agencies whose PKIs have cross-certified with the Federal Bridge CA (FBCA) at Medium-HW, or High Assurance Level may continue to assert department or agency-specific policy Object Identifiers (OID). Certificates issued on or after January 1, 2008 shall assert the id-CommonHW or id-CommonAuth policy OIDs. (Departments and agencies may continue to assert department or agency-specific policy OIDs in addition to the id-CommonHW and id-CommonAuth policy OIDs in certificates issued after January 1, 2008.)

Ms. Spencer said we might need to spin up the PD-VAL Working Group again. Maybe we did not go far enough, she said.

Cheryl Jenkins said she would put this before the FPKI Technical Advisory Group to see if we should spin up PD-Val or take another approach. She will inform the FPKIPA by next week what approach the MA would recommend.

Larry Shomo wondered if NIST would take on certification of PD-Val products. Ms. Spencer said NIST would only test if it were a NIST standard, but that GSA has a product evaluation and approval process.

Agenda Item 5

Briefing on the Proposed Triennial Compliance Audit Requirements—Jim Schminky

Jim Schminky (Treasury), chair of the Audit Working Group that developed the proposed new Triennial Compliance Audit methodology, briefed the FPKIPA on its purpose and requirements. He started by thanking the commercial auditor community who worked on the document, hand-in-hand with government auditors.

The intent of the “New Approach” is to make the audit process more palatable for all. It is a shift away from a one-time look at everything to a model of continuous monitoring, he said. The Audit Working Group (AWG) identified 50 core elements or requirements that would be reviewed each year. The core group represents approximately ¼ of all “Shall” statements in the RFC.

The first year in the cycle would be a full audit. The first year following the full audit would be a subset of RFC, representing roughly one third of the non-core controls, including a review of previous findings and any changes made during the year. Hence,

Year 1 = core elements, plus sections 1, 4, 7, 9 (plus previous findings, changes)

Year 2 = core elements, plus sections 2, 3, 5, 8 (plus previous findings, changes)

Year 3 = core elements, plus section 6 (plus previous findings, changes).

The new methodology requires the compliance auditor to address the Audit “Cook Book” or Compliance Audit Requirements, found on the Identity Management /FPKIPA website. The auditor would still audit the relevant controls in the client CP, which exceed those in the new methodology. For example, Treasury has nearly 500 “shall” statements or audit controls, and all would be audited over the three-year period—in conjunction with the core controls which are reviewed every year.

Ms. Spencer said this is an optional approach. The report states that the New Approach “shall be substituted for the previous requirement of a full compliance audit once every three (3) years and interim delta audits.”

Even if the FPKIPA finds this a viable alternative, she said, you would still have the option of doing a full annual audit.

Most non-federal and commercial entities and bridges require an annual audit. Many also utilize the Web Trust for CA (WTCA) methodology, which is based on an annual audit cycle. WTCA is the unofficial industry standard (recommended by the American Institute of Certified Public Accountants, or AICPA).

Nathan Faut (KPMG) said the WTCA is revising its requirements in Version 2.0 to bring them into alignment with the current FPKIPA Audit Cook Book. WTCA Version 2.0 is expected mid-year 2010.

Ms. Spencer said there is no one standard methodology for audits; indeed, there are many, including the US Federal Government, e-Valid8, T-Scheme and AICPA. If the FPKIPA approves the New Approach to auditing, it would be in the public domain and other entities would be welcome to use it, Ms. Spencer said. We might even consider promoting this as a new standard, she said. If the Federal Government adopts it, we would approach T-Scheme and AICPA/CICA

John Hannan (GPO) wanted to know how the Triennial Audit methodology aligns with the recognized standard of auditing, e.g., WTCA. Mr. Faut said that the Triennial Audit methodology is un-reconcilable with the WTCA approach. He said he would consult with GPO IG for its opinion.

Jim Schminky commented that the Triennial Audit methodology is un-reconcilable with the WTCA due to it being less than a full audit annually. The WTCA only recognizes a full and complete audit.

Ms. Spencer asked the FPKIPA to review the Triennial Audit methodology and submit their comments to the listserv before January 29, 2010. We should be prepared to vote on the Triennial Audit methodology at the 9 February 2010 FPKIPA meeting. She wanted to know if this methodology makes sense and if the core controls were correct. She noted that repositories (Section 2) are missing from the triennial lists and that the methodology currently references the FBCA CP, not the RFC.

Ms. Spencer also indicated she would approach Tony Cieri about briefing the IAB at its January meeting.

Ms. Spencer said this is one of the most important, if not the most important, thing we have done since we wrote the Common Policy. She encouraged all

FPKIPA members to make their views known by sending their comments to the FPKIPA listserv.

Ms. Fincher will send the Triennial Audit requirements document to the Forum of the Four Bridges for comment as well. (Done)

Agenda Item 6

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

1. Discuss / Vote: FCPF CP Change Proposal on Cryptographic Key Length

The FPKIPA voted to accept the FCPF CP Change Proposal on Cryptographic Key Length, which was recommended out of the CPWG by 11/14 or 78.6% where a ¾-majority vote was required. The purpose of this Change Proposal is to align the FCPF Policy with NIST SP 800-57, which calls for 3072-bit keys by 2030. The three “Absent” members had momentarily stepped away during the vote. A companion document for FBCA CP was approved at the December 2009 FPKIPA meeting.

Vote to approve FCPF CP Change Proposal on Cryptographic Key Length			
	Vote (Motion- Treasury 2nd- USPS)		
	Yes	No	Abstain
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	ABSENT		
Nuclear Regulatory Commission (NRC)	ABSENT		
SSA	ABSENT		
USPS	√		
USPTO	√		

2. Discuss / Vote: FBCA CP Change Proposal--CA Remote Administration

The FPKIPA voted to accept the FBCA CP Change on CA Remote Administration, which was recommended out of the CPWG, by 12/14, or 85.7% where a ¾-majority vote was required. The two “Absent” members had momentarily stepped away during the vote. The purpose of this Change Proposal is to accommodate the “lights out” operation of the FPKI MA, as part of the re-design, as well as other cross-certified Entities. The same security controls would be put on remote workstations used to administer a CA.

Vote to approve FBCA CP Change Proposal—CA for Remote Administration			
	Vote (Motion- DoS 2nd- NRC)		
	Yes	No	Abstain
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	ABSENT		
Nuclear Regulatory Commission (NRC)	√		
SSA	ABSENT		
USPS	√		
USPTO	√		

3. Discuss / Vote: FCPF CP Change Proposal—CA Remote Administration

The FPKIPA voted to accept the FCPF CP Change Proposal for CA Remote Administration, which was recommended out of the CPWG, by 12/14, or 85.7% where a ¾ majority vote was required. The two “Absent” members had momentarily stepped away during the vote. Mr. McBride said that remote workstations used to administer a CA would require two-person access controls, like the CA. Ms. Spencer noted this Change Proposal would apply to the FPKI MA and to the 6 COMMON entities, e.g., the Shared Service Providers.

Vote to approve FCPF CP Change Proposal—CA for Remote Administration			
	Vote (Motion- NRC 2nd- DoS)		
	Yes	No	Abstain
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	ABSENT		
Nuclear Regulatory Commission (NRC)	√		
SSA	ABSENT		
USPS	√		
USPTO	√		

Agenda Item 7

FPKI Management Authority (FPKI MA) Report--Cheryl Jenkins

Ms. Jenkins said that the monthly “DashBoard” report that went out early this morning contains information on Repository Usage, Redesign background and project schedule and other “highlights,” such as plans for a compliance audit on the current architecture.

The number of repository searches in December was approximately 26.3 million, and the repository availability was 100.0%. The new bandwidth is in place, DNS was switched last week, and improvements in performance should be noticeable.

Ms. Spencer stated that the funding for the re-design was approved and that OMB is tracking the FPKIA redesign.

Agenda Item 8

Other Agenda Items—Judith Spencer

PACS Demo—Ms. Spencer invited FPKIPA members and their contractors with PIV or CAC cards to a demo of PACS functionality at the Exostar location in Herndon, VA, on February 2. This R&D project was funded in part by GSA/ICAM, and as a result, the technical specifications will be made public. Attendees with PIV, CAC, PIV-I, and/or TWIC cards will be processed in advance via a GUI. Those credentials will be public key-enabled in advance for entrance into the building. CoreStreet (recently acquired by ActivIdentity) is providing the PKI PD-Val function. Contact Ms. Spencer for further information.

Agenda Item 9

Adjourn Meeting

Treasury made a motion to adjourn and Ms. Spencer adjourned the meeting at 11:50 a.m.

CURRENT ACTION ITEMS

No.	Action Statement	POC	Start Date	Target Date	Status
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

FPKIPA Minutes 12 January 2010 – Final

No.	Action Statement	POC	Start Date	Target Date	Status
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
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
378	Cheryl Jenkins will send out guidance to the agencies on how to use the various root stores.	Cheryl Jenkins	9 June 2009	14 July 2009	Open
379	Cheryl Jenkins will provide a milestone and timeline sheet for the redesign effort. This will be provided as a dashboard on a monthly basis to the FPKIPA.	Cheryl Jenkins	9 June 2009	14 July 2009 and monthly afterwards	Open
381	Judith Spencer will check with NIST for additional guidance on device certificates.	Judith Spencer	9 June 2009	18 June 2009	Open
382	Judith Spencer will talk with Bill Macgregor at NIST about guidance for Key Management history.	Judith Spencer	9 June 2009	18 June 2009	Open
382	Judith Spencer will send the Discussion Paper: "SSL Inspection and Mutual TLS Issue" to ICAMSC with today's date as an information paper, not a recommendation from the FPKIPA.	Judith Spencer	10 Nov. 2009	16 Nov. 2009	Open
383	The Secretariat will add a reference to the Discussion Paper: "SSL Inspection and Mutual TLS Issue," in the FY1010 Accomplishments paper.	Judith Spencer	10 Nov. 2009	Oct. 2010	Open
384	Wendy Brown is to draft an email memo for the ICAMSC re the Mozilla root store request and send to Brant Petrick for distribution to the ICAMSC.	Wendy Brown	10 Nov. 2009	16 Nov. 2009	Open
385	We need to write a Change Proposal, adding a <i>cardAuth</i> policy to FBCA. FBCA will require a UUID, as opposed to being optional.	Judith Spencer	10 Nov. 2009	30 Nov. 2009	Open

FPKIPA Minutes 12 January 2010 – Final

No.	Action Statement	POC	Start Date	Target Date	Status
386	Jim Schminky will provide the MA with a report of availability from a customer point of view, since Treasury does its own monitoring of availability of the FPKIA repositories.	Jim Schminky	10 Nov. 2009	30 Nov. 2009	Open
387	The Secretariat will put Debbie Mitchell's discussion of asserting Common Policy OIDS outside the <i>PIVauth</i> and <i>cardAuth</i> certificates for signature or encryption on the FPKIPA agenda for Dec. 8, 2009	Judith Fincher	10 Nov. 2009	8 Dec. 2009	Open