



Minutes of the 9 June 2009 Meeting

USPS, 475 L'Enfant Plaza, SW, Washington, DC
Conference Room 1P410
9:30 a.m. – 11:25 p.m.

A. AGENDA

1. Welcome / Introductions
2. Discuss/Vote on 12 May 2009 FPKIPA Minutes
3. FPKI PA Chair Nomination Process
4. FPKI Certificate Policy Working Group (CPWG) Report
5. FPKI Management Authority (FPKI MA) Report
6. ICAM BPA Contract Award
7. ICAMSC Update
8. Federal Delta Audit Parameters
9. Other Agenda Items
10. Adjourn Meeting

B. ATTENDANCE LIST

VOTING MEMBERS

The meeting began with a quorum of 13/15 (or 86.7%) 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.finch@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
Department of Homeland Security - revolving proxy	Miller, Tanyette	Teleconference
Department of Justice-Proxy to DoD	Proxy	Teleconference
Department of State	Gregory, Steve	
Department of Treasury	Schminky, Jim	
Drug Enforcement Administration (DEA CSOS)	Jewell, Chris	Teleconference

Organization	Name	Telephone
GPO	Hannan, John	Teleconference
GSA	Spencer, Judith	
NASA	Levine, Susan	Teleconference
Nuclear Regulatory Commission- NRC	Sulser, David	
SSA	ABSENT	
USPS	Stepongzi, Mark	
USPTO	Lindsey, Daniel	

OBSERVERS

Organization	Name	Telephone
Cipher Solutions, Inc.	Ahuja, Vijay	
FPKIPA Support/Secretariat (Contractor, Protiviti Government Services)	Fincher, Judy	
IdenTrust	Schambach, Marco	Teleconference
Treasury	Robinson, Michael	
GSA (Contractor, Unisys)	Petrick, Brant	
Department of State/ Co-chair, CPWG (Contractor, ManTech)	Froehlich, Charles	
GSA/OGP Support (RJ Schlecht Consulting)	Schlecht, R.J.	
Wells Fargo	Schwartz, Ruven	Teleconference
PM/FPKI MA/GSA	Jenkins, Cheryl	Teleconference
SSA (Contractor, Jacob & Sundstrom)	Jackmon, Kenya	Teleconference
FPKI MA Technical Liaison (Contractor, Protiviti Government Services)	Brown, Wendy	
DoE	Lonnerdal, Nils	
DoE	Varghese, Jebby	Teleconference
DoE	Olson, Evan	
DHS (Contractor, Protegus)	Shomo, Larry	Teleconference
USPTO	Kless, Patricia	Teleconference
FAA	Miller, Jayme	
FAA (Contractor, Covenant Security Solutions)	Kraus, Larry	
FAA (Contractor, Covenant Security Solutions)	DSouza, Darin	
FAA (Contractor, Covenant Security Solutions)	Patterson, David	
DOD (Contractor, Booz Allen Hamilton)	Neilson, Rebecca	Teleconference

C. MEETING ACTIVITY

Agenda Item 1

Welcome / Introductions—Judith Spencer, Interim Chair

The FPKIPA met at USPS Headquarters, 475 L'Enfant Plaza, SW, Washington, DC Conference Room 1P410. Judith Spencer, Interim Chair, called the meeting to order at

9:30 a.m. and conducted introductions of those present in person and via teleconference. We wish to thank Mark Stepongzi of USPS for hosting the meeting.

Agenda Item 2

Discuss/Vote on 12 May 2009 FPKIPA Minutes— Judy Fincher

The FPKIPA approved the redline 12 May 2009 FPKIPA minutes, unanimously (13/13) or 100%, where a 50% majority vote was required. Commerce and SSA were absent.

Approval vote for 12 May 2009 FPKIPA Minutes – red line version			
	Vote (Motion- Treasury, 2nd-USPS)		
	Yes	No	Abstain
Department of Commerce	ABSENT		
Department of Defense	√		
Department of Health & Human Services	√		
Department of Homeland Security	√		
Department of Justice – Proxy to DoD	√		
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 3

FPKI PA Chair Nomination Process—Judith Spencer

Ms. Spencer reported that she had received a nomination for the position of the FPKIPA Chair. She has been Interim Chair since July 2008. Ms. Spencer reported that David Sulser (NRC) nominated Jim Schminky of Treasury in an email of 8 June 2009. Should Mr. Schminky be unwilling or unable to serve, Mr. Sulser wishes to nominate Judy Spencer of GSA for Chair of the PA.

Nominations are open until COB June 11, 2009 and should be submitted to Judith Spencer in writing (e-mail)

Agenda Item 4

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

1. In-Person Antecedent Task Force

The CPWG at their 4 June meeting reviewed a new proposal from Jon Schoonmaker, Chair of the In-Person Antecedent Task Force. The CPWG found

it had merit and deserved to be brought before the Policy Authority. Jon Schoonmaker agreed to make changes to the existing documentation, to bring them in synch with the new language, concepts and process flow. The CPWG will review the revised materials at their next meeting on 16 June. Ms. Spencer said the documentation is intended to become supplemental guidance with pointers from within the CP. It is anticipated the FPKIPA will review this recommended guidance at the 14 July 2009 meeting.

2. DoD Audit Report

At the last CPWG meeting, John Cornell (GSA/Legal) expressed his concern with the apparent lack of independence of the National Security Agency (NSA) auditor of the Root CA. In the past the FPKIPA has accepted the IG of Civilian Agencies, as well as the DoD, as a legitimate auditor meeting the separation of duties criteria because most Federal IGs are appointed under the Inspector General Act of 1978 (5 USC App 3) as amended by the Inspector General Reform Act of 2008 (PL 110-409). As such, they have legal independence from all internal authorities. Mr. Cornell said he preferred to see an independent, third party auditor performing the PKI audits. Ms. Spencer said she wanted to make sure the auditor was not in the same chain of command as the PKI. Ms. Spencer drew an organizational chart on a flip chart, depicting the relationship between the Auditor, the DoD PKI PMO and its operational arm (DISA), based on a "wiring diagram" she received from Debbie Mitchell. The DoD Root is being run by NSA and is under the I5 Group. The auditor is also under the I5 Group (I51). The DoD PKI PMO headed by Morris Hymes is under the I5P NSA Group, but is also a DoD Acquisition Program.

Jim Schminky wanted to know if the I5 approves the budgets for all three groups. Ms. Mitchell said she was not sure and did not want to go into too much detail in a public meeting.

It was established that the issue is only with the DoD Root CA operated by NSA. The subordinate CAs are run by DISA and another group (a contractor) audits the sub-CAs.

Ms. Spencer said the FPKIPA could vote to accept the DoD audit as sufficient if it so chooses. The membership wanted to examine the wiring diagram before moving to a vote.

ACTION: Judith Spencer will send out the organizational "wiring diagram" from Ms. Mitchell to the FPKIPA voting members before the next FPKIPA meeting (14 July 2009).

Ms. Spencer said the CPWG had requested that she meet with NIST next week to discuss auditor independence issues.

3. Entrust Mapping Status

The CPWG continued its review of the Entrust mapping matrices on 4 June 2009 and submitted questions on eight "Partials" and one "Not Comparable" finding to Entrust for a response.

4. GPO 3647 Mapping effort

The CPWG is still waiting for comments on the GPO General Mapping Matrix from the GPO.

5. NIST SP 800-79 Mapping

R. J. Schlecht reported that NIST SP 800-79 and the Common Policy are closely aligned for PKI compliance audit regarding RAs for PIV card issuers.

He also said he has been in touch with the WebTrust audit community and that WebTrust 2.0 will be released in two months to better align with ANSI audit standards.

6. Charter and By-Laws Revision

This agenda item was tabled pending receipt of FPKIPA Chair nominations.

7. White Paper: The Realized Value of FPKI

Judith Fincher displayed the Executive Summary of the White Paper and said that PGS is still revising the last two chapters. PGS plans to send it out to the CPWG and FPKIPA this week. This version will not include Judith Spencer's edits. Ms. Spencer said this White Paper is the follow-on to "The Evolving Federal Public Key Infrastructure" that introduced the concept of the Federal Bridge. It will be submitted to the ICAMSC and from there to the ISIMC for approval. It will be published on the Web under the Federal CIO Council imprimatur, she said. She asked that FPKIPA members pay particular attention to the chapters on the qualitative and quantitative value of FPKI.

Agenda Item 5

FPKI Management Authority (FPKI MA) Report—Cheryl Jenkins

1. Commercial Root Stores

Wendy Brown said that efforts to get the Common Policy root into various commercial Root Stores (Mozilla, Microsoft, Adobe, and Apple) had stalled. Apple had indicated that the Common Policy Certificate would be in their next OS release, but they did not include it in Mac OS X v10.5.7. Apple plans to include it in the next available software update [no date provided].

Ms. Brown said that all the legal agreements are in place for the Common Policy certificate to be included in the Adobe AATL, but they have postponed its release from the initial May 27 planned date and will notify us when it happens.

Ms. Brown also noted later in the meeting that one of the criteria that most, if not all, of these Root Stores looked for was an audit comparable to the WebTrust model.

ACTION: Cheryl Jenkins will send out guidance to the agencies on how to use the various root stores.

2. Directory Outages

Ms. Brown said the reliability of the repository has greatly increased. There was only four outages [in the first Quarter of this calendar year]. Since our implementation of the load balancing solution in December 2008, security

incidents were reduced from an average of 25 per month in Q1FY-09 (68 total in Q1FY-09) to 1.3 average per month in Q2FY-09 (4 total incidents in Q2FY-09).

3. Business Impact Analysis

Cheryl Jenkins said that the BIA is not ready; Cheryl spoke with John Cornell about the risks of using a commercial site for the FPKIA “alternate” backup site. The BIA is under internal review and will be sent out after finalization. She announced she had acquired space (the basement) at 7th and D Street for the primary site and that the build-out is underway. Consequently, the backup site will have to be moved from 7th and D, where it is currently housed, to another location—not necessarily on another power grid. She is currently looking at the DoD (Finksburg) and Treasury (Westminster) sites and a commercial site.

4. Redesign

Ms. Jenkins said people are in training for the redesign and that she plans to start shipping equipment to the site for deployment by the end of the 2009 Calendar year. She expects to know in the next couple of weeks the impact on the schedule.

ACTION: 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.

Agenda Item 6

ICAM BPA Contract Award—Judith Spencer

Ms. Spencer said that seven vendors had been awarded Blanket Purchase Agreements (BPA) for the ICAM initiative. This umbrella contract is to replace the separate contracts for e-Authentication (which expired in January 09) and FPKIPA. The BPA may be open to other agencies, so other agencies might be able buy off it. It will include support for all Identity Management (IdM) initiatives, including FPKIPA. The first Task Order under the BPA is to replace the NIH contract which is set to expire on June 14, 2009. This Task Order has not yet been awarded. It is a firm fixed price vehicle. She assured the FPKIPA there would be no break in support to the PA.

Agenda Item 7

ICAMSC Update—Judith Spencer

Ms. Spencer reported on the activities of the ICAMSC working groups:

1. The Roadmap WG is ready for comments on the first draft of the Roadmap and ICAM Segment [As Is -To Be] architecture. It includes everything ICAM, including PKI. She asked the FPKIPA to review it carefully, as the contractor writing it does not know either PKI or the FPKI. The ICAMSC has one month to review it. It is the document agencies will use to develop their 2011 IdM budget. The ICAM segment architecture will go to the ICAMSC on June 15. Carol Bales reportedly wants to have it published by both the ISIMC and the ISC (Interagency Security Committee, the physical security folks).
2. The Citizen Outreach Focus Group is working with several credential provider schemes, including SAML and WS-federation, for schema adoption. The OpenID and InfoCard, recommendation is due out this month for Levels 1 and 2. A Level 3 one-time only password is under consideration. Levels 1 & 2 are being

- tested in the lab. The revised NIST SP 800-63 is not out yet. NIST may propose changes at levels 1 & 2 based on the work of the Citizen Outreach Focus Group.
3. Logical Access Control Systems (LACS) working group is looking at the PIV card for use at an agency's LACS. A guidance document is needed. That effort is being led by Bill Erwin (GSA) and Frank Jones (DoD) as the co-chairs. GSA will go live in 1-2 months with LACS, she said. Agencies that need guidance in moving to LACS need to help us focus that document on their questions and uncertainties.
 4. The Architecture Working Group (AWG) is addressing gaps in the Segment Architecture for ICAM. Their next meeting is 24 June 2009 at the White House Conference Center.
 5. DHS & DoD are working on backend attribute exchange for HSPD-12. They are using SAML to permit users to request additional authentication information, such as attributes, after their identification is confirmed. Six use cases are being piloted. Neal John of DHS has reported findings to the AWG.
 6. A "TAO of Attributes" workshop will be held this summer.

Agenda Item 8

Federal Delta Audit Parameters—Jim Schminky

Only one agency (DoD) responded in detail to Jim Schminky's request for comments on his proposal for updating the Federal Delta Audit Parameters. Steve Gregory from DOS provided an email requesting a cost benefit analysis. Mr. Schminky said a C/B analysis has not been performed because the list of prioritized controls [for the "core" set] does not exist.

Debbie Mitchell raised four questions and Mr. Schminky responded to each in turn during the meeting:

1. Does the focus of the audit become cloudy by splitting it into segments?

Mr. Schminky said that the PKI audit process will become uniform across all agencies and the "PKI environment." Far from clouding the issue, we will decide what will be reviewed each year: a core set of "shall" statements, plus 1/3 of the remaining security controls. Every three years you will have cycled through all the requirements. Every year we would address what has changed, as well as the documentation. We don't lose the continuity of the audit.

2. Will this facilitate a perception that federal agencies are held to different audit standards?

First, Mr. Schminky wanted to clear up a misunderstanding. This is not a "delta" audit proposal. The intent is to bring us back into annual audit compliance across the board. There is no two-tier membership. All cross-certified entities, including commercial, could use this standard. CertiPath is interested, Ms. Spencer said.

3. Do we need more detail in what is specifically being audited?

Mr. Schminky agreed more specificity is required. We haven't looked at the RA side at all, e.g., the core of identity management. Treasury found 499 security controls, for example, whereas there are only about 395 "shall" or "must" statements in Common, he said. If we're only doing "shall" or "must" statements, something is being left out. This new approach to auditing would apply to both Common and the FBCA, he said.

Moreover, Mr. Schminky said, we need to agree on the core PKI audit requirements. The FPKIPA members concurred and a special Audit Working Group will be set up to address Mr. Schminky's proposal and audit requirements under this new proposed schema. Mr. Schminky will lead the group. This group should include the commercial auditor community, especially WebTrust, the industry de facto standard PKI audit methodology. It was pointed out that Microsoft, Mozilla and Apple require a WebTrust audit as a pre-condition for inclusion in their root stores.

ACTION: R.J. Schlecht will re-convene the defunct Audit Working Group (AWG). (done)

The AWG will first develop a strawman before involving the external audit community. The process is intended for both federal and non-federal audits, and for both Common and FBCA.

Ms. Spencer said the PIV process requirements for audits are 1) 800-79 enrollment process, 3) triennial C&As.

4. Are the potential cost savings real?

Mr. Schminky then addressed the issue of the cost savings potential. Intuitively, it seems there would be a cost savings in being able to contract with the same auditor for a 3-4 year period, he said. That would eliminate the need to buy through three separate contract vehicles. He would like to see a BPA type contract so that all agencies could use the same group of auditors. Ms. Spencer suggested we might be able to use the GSA schedules to make it easier for the contract process.

Mr. Schminky said it would be impossible to come up with hard numbers regarding potential cost savings until the core set of auditable controls is identified. Perhaps the AWG should include a cost/benefit analysis in their scope.

Agenda Item 9

Other Agenda Items—Judith Spencer

a) 14 July FPKIPA Meeting Location

The FPKIPA needs to find a meeting location for the 14 July 2009 meeting. If no one comes forward, Brant Petrick will find a space at GSA. Steve Gregory said that he might be able to find a space at the nearby Department of State facility and will let us know.

- b) Nils Lonnerdal reported that the Department of Energy Senior Management (the CIO and Legal Department) are reviewing the revised CP. Once it is approved, they will submit it to the CPWG for mapping. Since the DoE is a legacy PKI, Carol Bales has agreed to let them renew their relationship to the Federal Bridge. They do not have to subordinate under Common, Ms. Spencer said. She asked the CPWG to put this mapping on their agenda for the fall.
- c) Ms. Spencer stated she is still planning to get the cross-certified legacy agencies to come in under Common. This would not be subordination, she said. Legacy PKI agencies running at Medium and above would cross-certify with Common.

For Rudimentary and Basic, the agencies would have to keep their cross-certificates with the FBCA, as would externally facing agencies, such as DEA CSOS, ACES, DoD ECA.

The rule is: for legacies with external constituencies, stay on the Federal Bridge. For legacies with internal constituencies, move to Common.

This is part of the FPKIA re-design, she said, noting this would occur no earlier than the January 2010 timeframe.

- d) Jayme Miller (FAA) joined the FPKIPA for the first time at this meeting. He was urged to make a formal application to the FPKIPA to become a voting member under the VeriSign SSP.

Mr. Miller reported on activities underway at the FAA to get PKI implemented in the operations part of the FAA, e.g., the National Air Space System. VeriSign is providing PKI for the PIV cards, but the FAA needs a solution for the whole access control suite of services. There will have to be a data exchange between the High Trust environment and their external constituents.

- e) Debbie Mitchell reported that DoD will soon start an interactive ECC unclassified pilot with RSA and hope to publish the results in September 2009. Wendy Brown added that the MA is working with DoD to test the ability of the redesign CA to issue cross certificates to an ECC CA.
- f) Debbie Mitchell also reported that DoD is doing a lot with device certificates and asked for further guidance on their use within the FPKI environment.

ACTION: Judith Spencer will check with NIST for additional guidance on device certificates.

- g) Ms. Spencer said that NIST is working on guidance for Key Management history.

ACTION: Judith Spencer will talk with Bill Macgregor of NIST about guidance for Key Management history.

Agenda Item 10

Adjourn Meeting—Judith Spencer

Ms Spencer adjourned the meeting at 11:25 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

FPKIPA Minutes 9 June 2009 FINAL

No.	Action Statement	POC	Start Date	Target Date	Status
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	
377	Judith Spencer will send out the organizational "wiring diagram" from Ms. Mitchell to the FPKIPA voting members before the next FPKIPA meeting (14 July 2009).	Judith Spencer	9 June 2009	15 June 2009	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