



Minutes of the 11 May 2010 Meeting
General Services Administration (GSA)
18th and F Streets, NW,
Washington, D.C.
9:30 a.m. – 11:42 a.m.

A. AGENDA

- 1. Welcome / Introductions**
- 2. Discuss / Vote on 9 March 2010 FPKIPA Minutes**
- 3. Discuss / Vote on 6 April 2010 FPKIPA Minutes**
- 4. Discuss / Vote on FBCA CP Change Proposal: 2010-xx (PIV-I)**
- 5. Discuss / Vote on Revised MOA Template for PIV-I**
- 6. FPKI Certificate Policy Working Group (CPWG) Report**
 - 1. Report on NIST SP 800-128 and OMB M-10-15 (Continuous Monitoring)**
 - 2. Mapping of NIST SP 800-53 version 3 to the FBCA CP**
 - 3. Mapping USPTO at Medium Hardware**
- 7. FPKI Management Authority (FPKI MA) Report**
- 8. Other Agenda Items**
 - *ICAM Report*
 - *Introduction of Deborah Gallagher*
- 9. 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. Two members joined later, via teleconference, bringing the total to 15/15 or 100% of voting members.

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

FPKIPA Meeting Minutes

Organization	Name	Telephone
Department of Justice	Morrison, Scott	
Department of State	McCloy, Mark	Teleconference
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
Veterans Administration (VA)	Jurasas, Eric	Teleconference

OBSERVERS

Organization	Name	Telephone
DHS (Designee GSA/ Office of Governmentwide Policy)	Gallagher, Debb	
GPO IG Audit Office (Ernst & Young)	Iijima, Timothy (T.J.)	
FPKI MA/PM	Jenkins, Cheryl	
FPKIPA Support	Louden, Chris	
Entrust (vendor)	Hernick, Nick	Teleconference
FPKI MA and FPKIPA Support (Contractor, Protiviti Government Services)	King, Matt	Teleconference
GSA Support (Contractor, Unisys)	Petrick, Brant	
DoS (Contractor, ManTech)	Froehlich, Charles	Teleconference
FPKIPA Secretariat (Contractor, Protiviti Government Services)	Fincher, Judy	
FPKIPA (Contractor, PGS)	McBride, Terry	
FPKI MA Technical Liaison (Contractor, Protiviti Government Services)	Brown, Wendy	
DOE (Contractor, M Squared Strategies, Inc.)	Olson, Evan	Teleconference
Cipher Solutions (vendor)	Ahuja, Vijay	Teleconference
eValid8 (Contractor)	Dilley, Brian	
CertiPath	Howard, Steve	Teleconference

C. MEETING ACTIVITY

Agenda Item 1

Welcome / Introductions—Judith Spencer, Chair

The FPKIPA met at the GSA Headquarters, 18th and F Streets, NW, Room 7300, Washington, D.C. Judith Spencer, 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 Judith Spencer of GSA for hosting this meeting.

Agenda Item 2

Discuss / Vote on 9 March 2010 FPKIPA Minutes—Judy Fincher

Ms. Fincher said the ICAM section of the 9 March 2010 FPKIPA minutes was now verified by Ms. Spencer and asked for a vote to approve the minutes. The minutes were approved by 13/15 (86.7%) where a 50% majority vote was required.

Approval Vote for 9 March 2010 FPKIPA Minutes			
Voting members	Vote (Motion – DoJ ; 2nd – GPO)		
	Yes	No	Abstain
Department of Defense	x		
Department of Health & Human Services	x		
Department of Homeland Security	x		
Department of Justice	x		
Department of State	x		
Department of the Treasury	x		
Drug Enforcement Administration (DEA CSOS)	x		
GPO	x		
GSA	x		
NASA	Absent for this vote		
Nuclear Regulatory Commission (NRC)	x		
SSA	x		
USPS	x		
USPTO	Absent for this vote		
Veterans Administration	x		

Agenda Item 3

Discuss / Vote on 6 April 2010 FPKIPA Minutes —Judy Fincher

Ms. Fincher circulated a redline version of the April 6 FPKIPA minutes prior to the meeting and asked the FPKIPA to approve the minutes as edited. The minutes were approved by 13/15 (86.7%) where a 50% majority vote was required.

Approval Vote for 6 April 2010 FPKIPA Minutes			
Voting members	Vote (Motion – NRC ; 2nd –USPS)		
	Yes	No	Abstain
Department of Defense	x		
Department of Health & Human Services	x		
Department of Homeland Security	x		

FPKIPA Meeting Minutes

Department of Justice	×		
Department of State	×		
Department of the Treasury	×		
Drug Enforcement Administration (DEA CSOS)	×		
GPO	×		
GSA	×		
NASA	Absent for this vote		
Nuclear Regulatory Commission (NRC)	x		
SSA	x		
USPS	×		
USPTO	Absent for this vote		
Veterans Administration	×		

Agenda Item 4

Discuss / Vote on FBCA CP Change Proposal: 2010-xx (PIV-I)—Judith Spencer, Terry McBride

The FPKIPA discussed the FBCA CP Change Proposal for PIV-I extensively at the meeting and in the end opted to do an e-vote, which is due COB May 18, 2010 to the listserv. Treasury made the motion to conduct an e-vote and DoD seconded.

Summary

Ms. Spencer said that the Change Proposal added three new Policy OIDs (id-fpki-certpcy-pivi-hardware, id-fpki-certpcy-pivi-cardAuth, id-fpki-certpcy-pivi-contentSigning) for use with PIV-I smart cards, and one new level of assurance, PIV-I Card Authentication, which is positioned between Medium and Medium Hardware.

PIV-Authentication is a level unto itself and is not yet covered in the FBCA, Ms. Spencer said.

David Sulser questioned the need for a specific PIV-I content signer policy. Why not just do one for all of Medium Hardware?

Jim Schminky wanted the FPKIPA and CPWG to consider including a content signing OID for PIV. Is there value/need to add one for PIV? he asked. Ms. Spencer acknowledged it was a mistake not to have done it also for PIV. That will be deferred to another Change Proposal, she said.

Judith Spencer indicated NIST is looking at FIPS 201 and perhaps we should ask NIST to add the PIV content signing OID.

She acknowledged having the content signing OID creates more work for providers who wish to be PIV-Interoperable, but that it is easier on the Relying Parties.

David Sulser: Why not treat all of Medium Hardware as a group and call it Med HW PIV-I-- as we did with Med HW CBP?

FPKIPA Meeting Minutes

John Hannan concurred. They are all Hardware credentials. PIV-I follows Medium Hardware except in 10-20 places, he said.

Terry McBride said the OIDs have already been registered with NIST, but that the friendly names could be changed.

The FPKIPA agreed to vote on it “as is” and debate the name change issue later. The FPKIPA agreed to two changes in the Change Proposal that David Sulser suggested. The practice note in 3.1.1 was removed and in 6.1.1.2, a reference to “PIV-I Card Authentication” was deleted. Debbie Mitchell said that DoD Senior Managers had the following comments:

1. They wanted country of citizenship added to the PIV-I card.
2. They requested two changes to the Profile document, which was done.
3. Regarding card topography, DoD wanted Zone 11 to be horizontal so it will not look like a PIV card.
4. They wanted to know what prevents them from using an agency name as their affiliation.

The first three DoD comments were acknowledged, as having been discussed and turned down during earlier discussions in the PIVITT and CPWG. The fourth DoD comment is already addressed in the FBCA CP 3.1.2 requirement for meaningful names not to be misleading.

Agenda Item 5

Discuss / Vote on Revised MOA Template for PIV-I— Judith Spencer, Debbie Mitchell, Jim Schminky

A sub-committee of the FPKIPA comprised of Ms. Spencer, Jim Schminky and Debbie Mitchell met on April 27 to revise the MOA template to accommodate PIV-I. The draft version was circulated last week and the final version, on Monday, May 10. Apart from the failure to define CP (Certificate Policy) and CPS (Certification Practices Statement) when first mentioned in 2 (b), there were no changes requested by the FPKIPA.

ACTION: Ms. Spencer will confer with John Cornell to see if he has any additional edits to the revised MOA template.

When Mr. Cornell weighs in the revised MOA template will be posted on the FPKIPA web site.

According to the FPKIPA Charter and By-Laws, no vote is required to amend the MOA template.

Agenda Item 6

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

a. Report on NIST SP 800-128 and OMB M-10-15 (Continuous Monitoring)—Charles Froehlich

This agenda item was tabled and will be discussed at the 8 June 2010 FPKIPA meeting.

Charles Froehlich encouraged the FPKIPA to look at the presentation on continuous monitoring that was distributed for this meeting. He said that the Department of State is looking into doing automated continuous monitoring.

Ms. Spencer said that Carl Crane (ISIMSC Information Systems Security Subcommittee) reports that a senior security program management subcommittee is working on new FISMA requirements in this area.

There was also some discussion --and differing views-- as to whether M-10-15 would apply to classified systems.

b. Mapping of NIST SP 800-53 version 3 to the FBCA CP—Terry McBride

Terry McBride reported that the CPWG has completed the mapping of NIST SP 800-53 version 3 to the FBCA CP, focusing on the new security controls in version 3, compared to the prior 800-53 mapping the CPWG performed in 2007. Each security control was rated: N/A, Comparable, Not Met, or Optional.

c. Mapping USPTO at Medium Hardware—Terry McBride, Judith Spencer

Terry McBride reported that the CPWG has started mapping the USPTO CP against the FBCA CP, using the original mapping matrices. PGS will present the mappings at Basic, Medium, and Medium Hardware at the 18 May CPWG meeting. Ms. Spencer said Cygnacom has already performed a mapping of USPTO using the original methodology.

In addition, PGS will conduct a trial mapping of the New Way Forward mapping methodology and present it to the CPWG on 3 June 2010. PGS is gathering metrics on the two approaches, to determine the amount of time required to do each type of mapping. The New Way Forward mapping has not yet been presented to the FPKIPA for approval.

The USPTO is waiting to receive the Medium HW cert from the FBCA before it begins issuing cards, according to Dan Lindsey, USPTO's representative on the FPKIPA. Ms. Spencer said you can issue cards

whenever, but there is no guarantee your policies will meet the FBCA CP until the mapping is completed.

Agenda Item 7

FPKI Management Authority (FPKI MA) Report--*Wendy Brown (for Cheryl Jenkins)*

- **Infrastructure Management**

Repository traffic continues to increase. There were 85 Million searches in the Repository in April, including over 48 million directory searches and over 37 million HTTP requests. To help maintain the improved repository performance with the increased traffic, the FPKI MA is deploying additional repository servers in addition to obtaining more bandwidth. There will be two repository sites by September and there are plans to add an additional three repository sites later.

Detailed repository usage statistics can be found on the Repository Dashboard, which was distributed to the listserv this morning.

- **OMB Passback Project**

New certificates do not have to be issued to all FBCA affiliates and SSPs by 9/30/2010, the "Go Live" date. However, the FPKI MA would like to start scheduling when we will issue new certificates between 9/30 and 12/31, as we would like to be able to decommission the current CAs before the end of the year. Wendy Brown will be contacting everyone to setup this schedule in the near future.

Please see the Passback Dashboard for status progress and highlights of this special project.

- **Security Management**

- **Compliance Audit**

GSA has an RFP in final review –not yet issued--for the following services:

- i. a retrospective audit on the current technical infrastructure,
- ii. a "Day Zero" on the Passback technical design, and
- iii. The NIST SP 800-53 system security accreditation.

Agenda Item 8

Other Agenda Items—Judith Spencer

1-ICAM Report

Ms. Spencer said the Federal Government needs to come up with a solution for the world for SHA 256. It needs more visibility, she said. She wants to know what the agencies' issues are with SHA 256. What products and patches have you tested to determine whether they are compliant with SHA 256? She asked. What products support it? She suggested the need for a survey of all the agencies.

Ms. Spencer said that the ICAM Logical Access Working Group meets on May 12 to discuss SHA 256 recommendations and that she has a meeting in June with NIST and Scott Jack (senior DoD Identity Management Official) to discuss this.

Microsoft's VISTA supports SHA 256, and XP will work via a patch. The best solution is to skip VISTA and go directly to Windows 7.

Wendy Brown said she will be advising Apple, Microsoft, Adobe, and Mozilla that we will be issuing a new Common Policy Root certificate signed with SHA 256, and will be requesting them to place this new root certificate in their respective trust lists. At that time, she will ask whether they know if this will create problems with their products.

Legacy applications will have problems. Bill Erwin (GSA) and Allison Scogin (DoD) have put together a SAML solution using Trust Bearer or Site Minder.

Ms. Spencer said an ICAM "Roadmap" update is in the works. She also said she is to write digital signature guidance for the PIV card, for Federal Agencies.

2-Introduction of Deborah (Debb) Gallagher

Ms. Spencer introduced Debb Gallagher. Ms. Spencer said Ms. Gallagher has accepted a position with GSA and will be taking on Ms. Spencer's responsibilities. She has worked for DoD and DHS and has a wealth of knowledge and experience, Ms. Spencer said.

Agenda Item 9

Adjourn Meeting

Ms. Spencer adjourned the meeting at 11:42 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
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	Ongoing
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	Closed
382	Judy 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 FY2010 Accomplishments paper.	Judith Spencer	10 Nov. 2009	Oct. 2010	Open

FPKIPA Meeting Minutes

No.	Action Statement	POC	Start Date	Target Date	Status
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
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
388	Cheryl Jenkins will reach out to Marianne Swanson (and Ron Ross) of NIST to determine what their audit standards strategy is vis-à-vis aligning the FBCA and NIST SP 800-53 with ISO standards.	Cheryl Jenkins	9 March 2010	13 April 2010	Open
389	Ms. Spencer will confer with John Cornell to see if he has any additional edits to the revised MOA template.	Judith Spencer, John Cornell	11 May 2010	14 May 2010	Open