



Minutes of the August 10, 2010 Meeting
GSA Headquarters
18th & F Streets Northwest, Conf Room 2239, Washington, DC
9:35 a.m. – 11:45 a.m.

A. AGENDA

1. Welcome / Introductions
2. Discuss/ Vote on 13 July 2010 FPKI Minutes
 - a. DOE Reinstatement
3. Legacy PKIs Move to Common - Status
4. SHA-256 Transition
 - Letter to CIOs / System Owners: Status
 - Collaborative Site: Brant Petrick
 - Real World Experience: Jim Schminky
 - Compile List of Products Issuing Patches to Support
 - SHA-256: Discussion Item
 - SHA 256 Working Sessions: Status
5. FPKI Certificate Policy Working Group (CPWG) Report
 1. Report from FPKI Security Profile WG: Status
 2. CertiPath PIV-I Mapping: Status
 3. VeriSign Mapping: Status
 4. Discuss / Vote on the following change proposals:
 - a. FBCA CP: Digitally Signed Declaration of Identity
 - b. FBCA CP: Real ID
 - c. Common CP: Archive Definition
 - d. EGCA: Align Operations with FBCA
 - e. C4CA: Align Operations with FBCA
6. FPKI Management Authority (FPKI MA) Report
7. Other Agenda Items
 - *ICAM Update – Judith Spencer*
 - *Next FPKI meeting, 14 September 2010*
8. Adjourn Meeting

B. ATTENDANCE LIST¹

Voting Members:

Organization	Name	Telephone
Department of Defense	O'Brien, Shawn (proxy for Mitchell, Debbie)	Teleconference
Department of Health & Human Services	Slusher, Toby	Teleconference
Department of Homeland Security	Miller, Tanyette (Proxy for Don Hagerling)	
Department of Justice	Morrison, Scott	
Department of State	Frahm, Jarrod M.	
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	Kless, Patricia	Teleconference
Veterans Administration (VA)	Miller, Jason (proxy for Eric Jurasas)	Teleconference

Observers:

Organization	Name	Telephone
NASA	Morris, Justin	Teleconference
GSA	Gallagher, Deb	
NIST	Cooper, Dave	Teleconference
Entrust	Moore, Gary	Teleconference
DoE	Breland, Mary Ann	
FPKIPA Support and Acting Secretariat (Contractor, Protiviti)	King, Matt	
GSA Support (Contractor, Unisys)	Petrick, Brant	
DoS (Contractor, ManTech)	Froehlich, Charles	
FPKIPA (Contractor, Protiviti)	McBride, Terry	
FPKIMA Technical Liaison (Contractor, Protiviti)	Brown, Wendy	
Cipher Solutions (vendor)	Ahuja, Vijay	Teleconference
DigiCert	Schambach, Marco	Teleconference
Ernst & Young	Iijima, Timothy	Teleconference
DoE	Olson, Evan	
SAFE Bio-Pharma	Schoonmaker, Jon	Teleconference

¹ Contact information was redacted in the published minutes at the request of FPKIPA members. This information will be posted to a secure website for FPKIPA members at some point in the future. FPKIPA minutes already posted on the website were redacted to remove POC information. FPKIPA members POC information on other members and participants should contact the Secretariat at Matthew.King@pgs.protiviti.com

Organization	Name	Telephone
EPA (Contractor)	Simonetti, Dave	
DOS (Contractor)	Jung, Jimmy	Teleconference

C. MEETING ACTIVITY

Agenda Item 1

Welcome / Introductions

Judy Spencer

The FPKIPA met at the GSA Headquarters located on 18th & F Streets NW, Conf. Rm. 2239, Washington DC. Judith Spencer, Chair, called the meeting to order at 9:35 A.M. and introduced those present in person and via teleconference.

Agenda Item 2

Discuss / Vote on 13 July 2010 FPKI Minutes

Matt King

Mr. King said that all changes had been made to the circulated July 13, 2010 FPKIPA minutes, and asked for a vote to approve the minutes. The minutes were approved by a 15/15 (100.0%) where a 50% majority vote was required.

Approval Vote for 13 July 2010 FPKIPA Minutes			
Voting members	Vote (Motion – GPO; 2 nd – 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	√		
Nuclear Regulatory Commission (NRC)	√		
SSA	√		
USPS	√		
USPTO	√		
Veterans Administration	√		

Agenda 2a

DOE Reinstatement

Judy Spencer

Judy Spencer added this agenda item during the meeting. Ms. Spencer explained that DOE was formerly an FPKIPA member and would like to rejoin the FPKI and reinvigorate their PKI. DOE is requesting (following up with a memo) to become re-cross certified with the federal bridge and be reinstated as a voting member of the FPKIPA.

Ms. Spencer then called for a vote to reinstate DOE.

David Cooper asked whether DOE's cross-certification with FBCA runs counter to M-05-05 and Ms. Spencer replied that normally his statement would be true, but DOE simply suspended operations and Judy spoke with Carol Bales to explain the situation and Ms. Bales had no objection. This vote is only to reinstate voting privileges so they can vote (on everything except their own cross-certification).

The vote to approve the reinstatement of DOE as a voting member of the FPKIPA passed with (15/15) 100.0% where a 75% majority is required:

Approval Vote for DOE Reinstatement			
Voting members	Vote (Motion – NRC; 2 nd – 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	√		
Nuclear Regulatory Commission (NRC)	√		
SSA	√		
USPS	√		
USPTO	√		
Veterans Administration	√		

ACTION: The DOE Cross-Certification application will be reviewed and voted on at the September 14, 2010 FPKIPA meeting

Agenda Item 3

Legacy PKIs Move to Common – Status

Judy Spencer

Judy Spencer provided an update on the issue of whether the Legacy Federal PKIs should move from the Bridge to cross-certify with Common. Ms. Spencer explained that she held a meeting with all Legacy Federal PKIs cross-certified with the FBCA to see if they wanted to cross-certify with Common to ease transition to PIV-I, shorten path length, etc.. Matt King explained that the Agency responses thus far were as follows:

Legacy Move to Common Responses (as of 9 August 2010)	
GPO	Remain on bridge
Treasury	Remain on bridge
DoD	Remain on bridge
State	Move to Common
USPS	Move to Common
USPTO	No Response Yet
Justice	No Response Yet

ACTION: Patricia Kless will discuss USPTO’s desire to Move to Common with Dan Lindsey and respond to the FPKIPA

Ms. Spencer then asked the group if we want to move those who want to move and leave those who want to stay. She explained that this would be a peer to peer cross-certification.

Wendy Brown explained that if agencies want to be recognized outside of Federal Government, they need to distribute their root – they wouldn’t need to do this if they cross-certified with Common.

Jon Schoonmaker stated that this seems to negate some value of the bridge, but Ms. Spencer responded that it actually reinforces the bridge’s role as building the relationship between the Federal Government and the external community. With PIV-I and the initiative for Cyber security we are seeing a growth in interest in cross-certifying with the FBCA. In addition, the EU, the UK, and Canada are looking to revive their PKIs and want harmonization, so the FBCA will be increasing its role.

Jim Schminky suggested that it might be reasonable to bring David Cooper’s idea to the table: since Common is now a hybrid, we could meld Common and Bridge into one activity. Ms. Spencer responded that the concept of Common and FBCA is that they will be separate and the degree of separation is useful. She added that we don’t want the FBCA to become an “uber-bridge”, but has had some discussions about transitioning from a hub-spoke model to a matrix model.

Mr. Schminky stated that the Matrix model is best to find the shortest path for PD-Val.

Ms. Spencer then suggested that Ms. Brown discuss with the MA whether there is a real compelling case to move those who want to Common, but the group agreed that the issue is more related to interoperability depending on which agencies communicate with each other.

ACTION: The issue of whether to move some of the Legacy Federal PKIs to Common will be discussed at the 17 August CPWG

ACTION: DOE will indicate their desire about whether to cross certify with the FBCA or Common

Agenda Item 4 SHA-256 Transition Judy Spencer

Judy Spencer provided an update on activities related to the SHA-256 Transition. Ms. Spencer stated that she got input from NIST on the SHA-256 Letter. Once the letter is finalized, Ms. Spencer will send it to the PA. The letter will be sent by the CIO Council on behalf of the FPKIPA and essentially notifies everyone running applications using PIV or PKI that this issue is coming and gives advice about what they can do to mitigate the impact of the transition to SHA-256.

Ms. Spencer noted that she has a request from SAFE for an extension to June 2011, because they use Juniper for their VPN and Juniper is developing a patch (which is not yet final). Johnson & Johnson (J&J), a SAFE member, received a beta patch from Juniper, but it did not work. Juniper promised they would get a working patch before year end. Because J&J is a global organization it needs 6 months to test and do a worldwide transition. Ms. Spencer suggested that if an agency intends to ask for an extension, they need to submit a plan detailing the reason for the extension with clear steps on when the plan will be completed.

Ms. Spencer also noted that she has received a change proposal requesting relief of the SHA-256 requirement for three years, but it is not expected that the change proposal would be viable, since it goes against NIST requirements stated in 800-78 and 800-131.

ACTION: Ms. Spencer agreed to send additional clarification about requirements surrounding SHA-256 that appear in NIST SP 800-78, 800-131, and other related Special Publications.

Brant Petrick provided a description of the collaborative web site established to share information about the SHA-256 transition.

ACTION: Brant will send information to the FPKIPA mail list about how to access the SHA-256 Collaborative web site.

Jim Schminky provided an overview of Treasury's efforts to plan for the SHA-256 Transition and referenced the briefings distributed to the FPKIPA prior to the meeting. Susan Levine mentioned that NASA has also performed testing and will post their information to the web site. Additional discussion was held about specific SHA-256

product issues. The SHA-256 weekly collaboration and planning discussions are now being held to provide the community the opportunity to share information related to the transition.

ACTION: Wendy Brown will send an e-mail informing agencies that she will accept and respond to requests for test CA certificates with either SHA-1 or SHA-256 for testing.

Agenda Item 5

FPKI Certificate Policy Working Group (CPWG) Report

Charles Froehlich / Terry McBride

Report from FPKI Security Profile WG: Status

Terry McBride explained that they are halfway thru identifying FPKI guidance for implementation of security controls and are hoping to finish review of those controls in the next meeting (11 August 2010). The next phase will review how the controls will be assessed in alignment with NIST SP 800-53A

CertiPath PIV-I Mapping: Status

The CPWG reviewed the mapping and there are a few issues about which we need their response. Mr. McBride explained that he is hopeful that we can resolve these issues at the next CPWG meeting

VeriSign Mapping: Status

Mr. McBride stated that the VeriSign mapping completed and there a few more steps before we recommend acceptance by PA (e.g., PIV-I card testing).

Discuss / Vote on the following change proposals:

a. FBCA CP: Digitally Signed Declaration of Identity

DoD stated that they needed additional time to review and comment on this change proposal. Therefore, the discussion and vote of the change proposal for Digitally Signed Declaration of Identity was deferred and will be discussed at the next CPWG meeting. Following any revisions, this change proposal will be forwarded to the FPKIPA voting members for electronic vote.

b. FBCA CP: Real ID

The purpose of this change is to add a Real I.D. Act compliant Picture I.D. to the list of acceptable credentials when doing Identification of Human subscribers. Judy Spencer provided some background on REAL ID and DHSs role in bringing this issue to the

CPWG. Ms. Spencer explained how a star and circle logo will be used to indicate if a REAL ID is compliant.

David Sulser from NRC asked about accepting expired credentials and Ms. Spencer explained that it is not desirable to accept credentials that are not current and valid. Slight modifications were made to the change proposal based on discussion about the specific meaning of the proposed language.

The vote to approve the change proposal for Real ID passed with (15/16) 93.7% where a 75% majority is required:

Approval Vote for FBCA CP Change Proposal: 2010-xx (Real ID)			
Voting members	Vote (Motion – Treasury; 2nd – DOJ)		
	Yes	No	Abstain
Department of Defense	√		
Department of Energy	√		
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	√		
USPS	√		
USPTO	√		
Veterans Administration	√		

c. Common CP: Archive Definition

The purpose of this change is to clarify the purpose of archiving, and the archiving requirements for auditable events. Terry McBride explained that the next few change proposals are about aligning other policies with recent changes to the FBCA CP so operations of the FPKI CAs is easier and consistent.

The vote to approve the change proposal for Archive Definition passed with (16/16) 100.0% where a 75% majority is required:

Approval Vote for Common CP Change Proposal: 2010-xx (Archive Definition)			
Voting members	Vote (Motion – Treasury; 2nd – DOJ)		
	Yes	No	Abstain
Department of Defense	√		

Approval Vote for Common CP Change Proposal: 2010-xx (Archive Definition)			
Voting members	Vote (Motion – Treasury; 2nd – DOJ)		
	Yes	No	Abstain
Department of Energy	√		
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	√		
USPS	√		
USPTO	√		
Veterans Administration	√		

d. EGCA: Align Operations with FBCA

The purpose of this change is to bring the EGCA CP into operational alignment with the FBCA CP. The vote to approve the change proposal to Align Operations with FBCA passed with (16/16) 100.0% where a 75% majority is required:

Approval Vote for EGCA CP Change Proposal: 2010-xx (Align Operations with FBCA)			
Voting members	Vote (Motion – USPS; 2nd – DHS)		
	Yes	No	Abstain
Department of Defense	√		
Department of Energy	√		
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	√		
USPS	√		
USPTO	√		
Veterans Administration	√		

e. C4CA: Align Operations with FBCA

The purpose of this change is to bring the C4CA CP into operational alignment with the FBCA CP. The vote to approve the change proposal for Align Operations with FBCA passed with (16/16) 100.0% where a 75% majority is required:

Approval Vote for C4CA CP Change Proposal: 2010-xx (Align Operations with FBCA)			
Voting members	Vote (Motion – USPS; 2 nd – GPO)		
	Yes	No	Abstain
Department of Defense	√		
Department of Energy	√		
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	√		
USPS	√		
USPTO	√		
Veterans Administration	√		

Agenda Item 6

FPKI Management Authority (FPKI MA) Report

Cheryl Jenkins

Cheryl Jenkins provided an update on MA activities in the last month. She stated that she made a trip to the West to tour a number of Federal and Commercial data centers. She found significant differences between Federal and Commercial data centers, which leads to concern about requirements to house components in Federal space. Ms. Jenkins requested a Feds Only meeting to discuss this concern.

ACTION: Matt King will schedule a Feds Only meeting to discuss concern about requirements to house components in Federal space after Ms. Spencer and Ms. Jenkins determine a time and day for the meeting.

Ms. Jenkins then provided an overview of the Redesign Dashboard. She mentioned that one of the components currently in Federal space will move to the West Coast. She also mentioned that the Security Management activity is behind schedule due to issues with the acquisition package. The good news is that award will be soon and the

retrospect audit will be started as soon as possible. The retrospect audit will then be leveraged for the C&A.

Ms. Jenkins then provided an overview of the Repository Dashboard. She noted that the FPKI had over 84 million and 79 million hits over LDAP and HTTP respectively – a total of over 163 million requests and a 90% increase since June. She pointed out that the infrastructure was able to respond, but there is still room for improvement, which will be reflected in the next month's dashboard. Ms. Jenkins also mentioned that she has requested the maximum bandwidth from each facility since there are too many unknowns related to the total volume of traffic. Ms. Spencer then quoted Dennis Fisher saying "the only thing we have to fear is success."

Agenda Item 7

Other Agenda Items

Judy Spencer

ICAM Update

Last month there was a meeting at NIST about the intention to revise FIPS 201. About 50 people attended the meeting and 7-8 key topics were discussed. The decision to revise FIPS 201 is still in process, but everything is progressing as expected. Ms. Spencer reminded the group that it still takes 18 months to go through the document revision process, so there will not be a new FIPS 201 document for at least 2 years.

Ms. Spencer also mentioned that additional progress is being made on the ICAM Roadmap and Implementation Guidance document. She noted that members of the FPKIPA may be called upon to discuss lessons learned and provide input to the roadmap about PKI technology and policy.

Next FPKI meeting, 14 September 2010

Agenda Item 8

Adjourn Meeting

Treasury (Mr. Schminky) made the motion to adjourn, and Ms. Spencer adjourned the meeting at 11:45 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-Jun-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-Oct-2008	12-Nov-2008	Open
378	Cheryl Jenkins will send out guidance to the agencies on how to use the various root stores.	Cheryl Jenkins	9-Jun-2009	14-Jul-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-Jun-2009	14 July 2009 and monthly afterwards	Ongoing
381	Judith Spencer will check with NIST for additional guidance on device certificates.	Judith Spencer	9-Jun-2009	18-Jun-2009	Open
382	Judith Spencer will talk with Bill Macgregor at NIST about guidance for Key Management history.	Judith Spencer	9-Jun-2009	18-Jun-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

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-Mar-2010	13-Apr-2010	Open
392	Update the application for cross certification to specify a Federal sponsor was not required if there was a clear indication that the application for cross certification was still in the interest of the Federal government	Brant Petrick	13-Jul-2010	15-Aug-2010	Closed
393	Patricia Kless will discuss USPTO's desire to Move to Common with Dan Lindsey and respond to the FPKIPA	Dan Lindsey	10-Aug-2010	14-Sep-2010	Open
394	DOE will indicate their desire about whether to cross certify with the FBCA or Common	Mary Ann Breland	10-Aug-2010	14-Sep-2010	Open
395	The issue of whether to move some of the Legacy Federal PKIs to Common will be discussed at the 17 August CPWG	Matt King	10-Aug-2010	17-Aug-2010	Closed
396	Ms. Spencer agreed to send additional clarification about requirements surrounding SHA-256 that appear in NIST SP 800-78, 800-131, and other related Special Publications	Judith Spencer	10-Aug-2010	14-Sep-2010	Open
397	Send information on SHA-256 Collaborative Site to PA List	Brant Petrick	10-Aug-2010	20-Aug-2010	Closed

No.	Action Statement	POC	Start Date	Target Date	Status
398	Wendy Brown will send an email notifying interested parties that she will accept and respond to requests for test CA certs with either SHA-1 or SHA-256 for testing	Wendy Brown	10-Aug-2010	14-Sep-2010	Open
399	Matt King will schedule a Feds Only meeting to discuss concern about requirements to house components in Federal space after Ms. Spencer and Ms. Jenkins determine a time and day for the meeting	Matt King	10-Aug-2010	20-Aug-2010	Closed
400	The DOE Cross-Certification application will be reviewed and voted upon at the September 14, 2010, FPKIPA meeting	Matt King	10-Aug-2010	14-Sep-2010	Open