



Minutes of the September 14, 2010 Meeting  
USPS Headquarters  
475 L'Enfant Plaza SW, Conf Room 4841, Washington DC 20001  
09:35 – 12:15 p.m.

**A. AGENDA**

1. Welcome / Introductions
2. Discuss / Vote on 10 August 2010 FPKIPA Minutes
3. Legacy PKIs Move to Common - Status
4. SHA-256 Transition
  - Letter to CIOs / System Owners: Status
  - SHA 256 Working Sessions: Status
5. Discussion / Vote: Use of SIA Extension
6. Discussion / Vote on DOE Cross – Certification Application
7. Discuss / Vote on Entrust PIV-I Application
8. FPKI Certificate Policy Working Group (CPWG) Report
  - Report from FPKI Security Profile WG: Status
  - Discuss / Vote CertiPath PIV-I Mapping Recommendation
  - Discuss / Vote VeriSign Mapping Recommendation
  - Discuss / Vote Digitally Signed Declaration of Identity change proposal
9. FPKI Management Authority Report
10. Other Agenda Items
  - Use of Wireless CA/RA Components
  - Facility Security Requirements
  - Next FPKIPA meeting, 12 October 2010

## A. ATTENDANCE LIST<sup>1</sup>

Voting Members:

Organization	Name	Telephone
Department of Defense	O'Brien, Shawn (proxy for Debbie Mitchell)	Teleconference
Department of Energy	Agee, Bonita (for MaryAnn Breland)	Teleconference
Department of Health & Human Services	Slusher, Toby	
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	Verdun, Thomas	
USPTO	Lindsey, Dan	
Veterans Administration (VA)	Jurasas, Eric	

Observers:

Organization	Name	Telephone
Cipher Solutions (vendor)	Ahuja, Vijay	Teleconference
DOE	Boysen, Brian	
FPKIMA Technical Liaison (Contractor, Protiviti)	Brown, Wendy	
NIST	Cooper, Dave	
DoS (Contractor, ManTech)	Froehlich, Charles	
Ernst & Young	Iijima, Timothy	Teleconference
GSA, FPKIMA PM	Jenkins, Cheryl	
DoS (Contractor, VertexTM)	Doty, R Lee	
DoS (Contractor, Slandala)	Jung, James	
Entrust	Moore, Gary	
DoE	Olson, Evan	
GSA Support (Contractor, Unisys)	Petrick, Brant	Teleconference

## B. MEETING ACTIVITY

<sup>1</sup> 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

**Agenda Item 1**

**Welcome / Introductions**

**Judith Spencer**

The FPKIPA met at the USPS Headquarters located at 475 L'Enfant Plaza SW, Conf. Rm. 4841, Washington, DC. Judith Spencer, Chair, called the meeting to order at 9:35 A.M. and introduced those present both in person and via teleconference.

**Agenda Item 2**

**Discuss / Vote on 10 August 2010 FPKIPA Minutes**

**Matt King**

Mr. King informed the Policy Authority that all changes have been made to the circulated August 10, 2010 FPKIPA minutes. The minutes were approved by a 15/15 (100.0%) vote where a 50% majority vote was required.

<b>Approval Vote for 10 August 2010 FPKIPA Minutes</b>			
<b>Voting members</b>	<b>Vote (Motion – Treasury ; 2<sup>nd</sup>–State)</b>		
	<b>Yes</b>	<b>No</b>	<b>Abstain</b>
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	Absent		
Veterans Administration	√		

**Agenda Item 3**

**Legacy PKIs Move to Common – Status**

**Judith Spencer**

Ms. Spencer stated she still believes that there is an advantage to moving Legacy PKIs under Common, however there are some Legacies that want to stay cross certified with the FBCA, some wanted to move and others did not express a strong desire either way. Terry McBride has prepared a change proposal for the Certificate Policy Work Group (CPWG) review that will allow Legacy PKIs to cross-certify (peer-to-peer mapping) with the Common CA. We will vote on it next month after the CPWG has reviewed it.

**Agenda Item 4**  
**SHA-256 Transition**  
**Judith Spencer / Matt King**

**a. Letter to CIOs / System Owners: Status**

Ms. Spencer requested feedback from the PA community regarding the SHA 256 memorandum. She only received responses from the State Department and Wendy Brown by the deadline. The group agreed that Ms. Spencer should finalize and distribute the memo.

**b. SHA 256 Working Sessions: Status**

An update regarding the SHA-256 transition was provided to the FPKIPA. Matt King informed the PA that the CPWG has created a spreadsheet narrowing the list of PK-enabled products in use that do not yet support SHA-256 and have no known resolution. He informed the group that the SHA-256 WG will continue to finalize the spreadsheet and ensure its accuracy.

Mr. Schminky inquired if the SHA-256 WG will be ready to present their findings to the PA by October. NIST will be hosting a meeting on SHA-256 in October. The SHA-256 WG plans to have this action complete by September 30<sup>th</sup>.

The risk of continuing to use SHA-1 was also discussed. Ms. Debbie Mitchell suggested that the FPKI Community needs to look at the risk of going to SHA-256 and not being able to validate things properly because of lack of vendor support for some products and evaluate which risk is greater.

Ms. Spencer explained to PA that if agencies are concerned they require additional time from NIST, they must submit a document describing the issue, proposed resolution, and timeline for implementation by the end of the month. This is the second time Ms. Spencer has requested this documentation. However, thus far only SAFE and SSA have provided feedback. Ms. Spencer continued to explain that NIST will not grant extensions without written documentation of the problem and a suggested mediation.

**Agenda Item 5**  
**Discussion / Vote: Use of SIA Extension**  
**Judith Spencer**

Judy Spencer summarized the decision to make the SIA extension optional within PKI until 2010 and gave her interpretation that this meant the end of 2010 vs. the interpretation of Dave Cooper that this meant the beginning of 2010. It was noted that the SIA extension had remained mandatory in the certificate profiles; and the decision to

make it optional was addressed only in the various PKI certificate policies. There was a very short discussion of the fact that Microsoft has “fixed” their handling of SIA by changing the default behavior of Microsoft products to ignore this extension and will now allow a certificate in their Trust Store to contain the extension. There was a quick poll to see if anyone objected to making the extension mandatory again. No one objected, although a few who have recently rekeyed said they needed to go back and check if they can add it. Therefore, the unedited certificate profiles will remain. However, Dave Cooper pointed out that SIA had been made optional in the PIV-I profiles and that might need to be changed.

**ACTION:** Cheryl Jenkins will draft a SOP for the PA regarding how to enforce correction of issues found in FPKI repositories and then forward a draft to CPWG.

### Agenda Item 6

#### Discussion / Vote on DOE Cross – Certification Application Judith Spencer

The Department of Energy is a Legacy member. The motion was opened by Treasury and seconded by State Department.

The DOE cross-certification application was approved by a 15/15 (100.0%) vote where a 50% majority vote was required

Approval Vote for DOE Cross-Certification Application			
Voting members	Vote (Motion – Treasury; 2 <sup>nd</sup> – State)		
	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 7

### Discuss / Vote on Entrust PIV-I Application

Judith Spencer

Entrust submitted an application to cross certify with the FBCA at PIV-I. It was noted that they are already cross-certified at Medium Hardware The motion was initiated by GPO and seconded by NRC.

Ms. Debbie Mitchell asked about the PIV-I roadmap and suggested that the testing scheme must be finalized and agreed upon before testing starts.

The Entrust PIV-I cross-certification application was approved by a 16/16 (100.0%) vote where a 50% majority vote was required.

Approval Vote for Entrust PIV-I Application			
Voting members	Vote (Motion – GPO; 2 <sup>nd</sup> – NRC)		
	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 8

### FPKI Certificate Policy Working Group (CPWG) Report

Charles Froehlich / Terry McBride

Charles noted that the SAFE-BioPharma audit letter was reviewed and there were no issues.

#### a. Report from FPKI Security Profile WG - Status

The Security Profile WG is continuing development of the FPKI Security Controls Profile. They are approximately one third of the way through the assessment phase. They have consulted with Ron Ross, NIST, and received positive feedback. The Security Profile WG will meet again on 16 September. Once the FPKI Security Controls Profile is approved by the FPKIPA, it will go to NIST for feedback and then to OMB for final approval.

### **b. Discuss/Vote CertiPath PIV-I Mapping Recommendation**

Terry McBride informed PA that CPWG has finished its review of the CertiPath mapping. All identified issues have been resolved. The CPWG recommends acceptance of CertiPath's PIV-I mapping.

The test plan for PIV-I still has to be reviewed and accepted, so no vote is necessary at this time.

### **c. Discuss/Vote VeriSign Mapping Recommendation**

Terry McBride informed PA that CPWG has finished its review of the VeriSign mapping. All identified issues have been resolved. The CPWG recommends acceptance of VeriSign's PIV-I mapping.

The test plan for PIV-I still has to be reviewed and accepted, so no vote is necessary at this time.

Terry McBride explained that ad hoc testing was planned while waiting for modified 85B test tool, but it doesn't look like the tool will be modified soon and that approach may not be enough. In addition there is a desire to add path testing to the test. The test plan will be submitted to and reviewed by the CPWG when it is ready.

### **d. Discuss/Vote Digitally Signed Declaration of Identity change proposal**

Mr. Froehlich presented a revised version of this change proposal. The CPWG was not able to reach consensus for the wording of this change proposal. Therefore, it has brought the current version to the PA for discussion.

Mr. Froehlich explained that the question whether signatures could be handwritten or digital was one of the reasons it was referred back to the CPWG. DoD (CPMWG) proposed either a handwritten signature or biometric (e.g., fingerprint), or both, so there is an established link to the person actually signing. SAFE-BioPharma recommended different wording. The revised version incorporated a portion of SAFE's proposal, but this change to the Change Proposal was deemed to be too vague. Additional discussion regarding the need for "wet ink" signatures; the need to introduce biometrics as a requirement into the FBCA CP given that an increasing number of cross certified members were not Federal or even governmental Entities; and, potential alternatives to both was held. It was agreed that the language needed review by legal counsel for interpretation.

**ACTION:** Judy Spencer will consult Tom Smeddinghoff, John Cornell and Shauna about the meaning of the language proposed in the change proposal.

**Agenda Item 9  
FPKI Management Authority Report  
Cheryl Jenkins**

Cheryl Jenkins informed the PA that the Management Authority is in the process of completing its audit and it is expected that the audits will be complete by 6 October. She noted that they have questions regarding Trusted Internet Connections (TIC), and inquired if the CPWG has drafted the letter deciding what the stance will be for the PKI TIC connection.

**ACTION:** FPKI MA will draft a memo about Trusted Internet Connection (TIC) and PKIs for consideration by the CPWG.

**Agenda Item 10  
Other Agenda Items  
Judith Spencer**

**a. Use of wireless CA/RA Components**

Ms. Spencer noted that the certificate policies were originally written in 2002, wireless was not as prevalent as it now is. Moving forward we may require specific language addressing wireless and requested this issue be discussed in the CPWG.

**b. Facility security requirements**

Last month Ms. Spencer held a meeting with the federal community and discussed the requirement to house the FPKI in federal buildings. The outcome on that meeting was that the MA will put together the actual facility security requirements and bring that back to the PA.

**c. Next FPKIPA meeting – 12 October 2010**

The meeting adjourned at 12:15 P.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

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-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
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

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
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
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

No.	Action Statement	POC	Start Date	Target Date	Status
401	Cheryl Jenkins will draft a SOP for the PA regarding how to enforce corrections for problems in the FPKI repositories and then forward a draft to CPWG	Cheryl Jenkins	14-Sep-2010	12-Oct-2010	Open
402	Judy Spencer will consult Tom Smeddinghoff, John Cornell and Shauna about the meaning of the language proposed in the Digitally Signed Declaration of Identity change proposal	Judith Spencer	14-Sep-2010	12-Oct-2010	Open
403	FPKI MA will draft a memo about Trusted Internet Connection (TIC) and PKIs for consideration by the CPWG	FPKIMA	14-Sep-2010	12-Oct-2010	Open