



**Minutes of the 8 December 2009 Meeting**  
**USPS, 475 L'Enfant Plaza, SW, Washington, DC.**  
**CR 2P316 (inside CR 2P310)**  
**9:45 a.m. – 11:05 a.m.**

**A. AGENDA**

- 1. Welcome / Introductions**
- 2. Discuss/Vote on 10 November 2009 FPKIPA Minutes**
- 3. Discuss Asserting COMMON Policy OIDs outside of PIVauth and cardAuth for signature or encryption**
- 4. FPKI Certificate Policy Working Group (CPWG) Report**  
 1- *Discuss / Vote : FBCA CP Change Proposal on Cryptographic Key Length*
- 5. Discuss / Vote to approve the Entrust Managed Service SSP Audit**
- 6. FPKI Management Authority (FPKI MA) Report**
- 7. 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. USPTO was absent for the fourth time in a row.

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.Fincher@pgs.protiviti.com](mailto:Judith.Fincher@pgs.protiviti.com).

<b>Organization</b>	<b>Name</b>	<b>Telephone</b>
Department of Defense	O'Brien, Shawn	Teleconference
Department of Health & Human Services	Slusher, Toby	Teleconference
Department of Homeland Security	Miller, Tanyette	Teleconference
Department of Justice	Morrison, Scott	
Department of State	McCloy, Mark	
Department of Treasury	Schminky, Jim	
Drug Enforcement Administration (DEA CSOS)	Jewell, Chris	Teleconference
GPO	ABSENT	
GSA	Spencer, Judith	
NASA	Levine, Susan	Teleconference

<b>Organization</b>	<b>Name</b>	<b>Telephone</b>
Nuclear Regulatory Commission- NRC	Sulser, David	
SSA	Mitchell, Eric	Teleconference
USPS	Stepongzi, Mark	
USPTO	ABSENT	

**OBSERVERS**

<b>Organization</b>	<b>Name</b>	<b>Telephone</b>
Entrust (vendor)	Moore, Gary	
FPKI MA/PM	Jenkins, Cheryl	
FPKI MA (PGS, Contractor)	Louden, Chris	Teleconference
IdenTrust	Schambach, Marco	Teleconference
FPKI MA (PGS, Contractor)	Pinegar, Tim	Teleconference
GSA Support (Contractor, Unisys)	Petrick, Brant	
Department of State/ Co-chair, CPWG (Contractor, ManTech)	Froehlich, Charles	
GSA Support (Consultant, RJ Schlecht Consulting)	Schlecht, R.J.	
FPKI PA (Contractor, PGS)	McBride, Terry	
FPKI MA Technical Liaison (Contractor, Protiviti Government Services)	Brown, Wendy	
GPO/Office of the Federal Registrar	Massimini, Mike	Teleconference
Cipher Solutions (vendor)	Ahuja, Vijay	Teleconference
eValid8 (vendor)	Dilley, Brian	
NASA	Baldrige, Tim	
DHS (Contractor)	Shomo, Larry	
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

**Agenda Item 2****Discuss/Vote on 10 November 2009 FPKIPA Minutes—Terry McBride**

The 10 November 2009 FPKIPA Minutes will be voted on at the 12 January 2010 meeting, since Ms. Fincher was not present to comment on any changes/edits to those minutes. (There were none.)

### Agenda Item 3

#### Discuss Asserting COMMON Policy OIDs outside of PIVauth and cardAuth for signature or encryption—Debbie Mitchell

This item was not discussed at length due to Ms. Mitchell's absence. It will be on the agenda for the 12 January FPKIPA meeting, when she can participate.

### Agenda Item 4

#### FPKI Certificate Policy Working Group (CPWG) Report—Charles Froehlich, Terry McBride

##### 1. Discuss / Vote: FBCA CP Change Proposal on Cryptographic Key Length—Charles Froehlich

The FPKIPA voted to accept the FBCA CP Change Proposal on Cryptographic Key Length, which was recommended out of the CPWG. The purpose of this Change Proposal is to align the FBCA Policy with NIST SP 800-57, which calls for 3072-bit keys by 2030. The CPWG will discuss a companion Change Proposal for COMMON at its December 14, 2009 meeting, for a vote by the FPKIPA on January 12, 2010.

Vote to approve FBCA CP Change Proposal on Cryptographic Key Length			
	Vote (Motion- NRC 2 <sup>nd</sup> - State)		
	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)	√		
SSA	√		
USPS	√		
USPTO	ABSENT		

The CPWG is working on two other Change Proposals, which should come before the FPKIPA in January. They are the FBCA and COMMON Change Proposals for remote administration of CAs. A third Change Proposal to support the Triennial Compliance Audit approach is also being worked and should be ready for a vote by the FPKIPA in February 2010.

**Agenda Item 5**

Discuss / Vote to Approve the Entrust Managed Service SSP Audit —John Cornell

John Cornell, FPKIPA legal counsel, presented his evaluation of the Entrust Managed Service SSP Audit, which was performed by eValid8. The auditor “dinged” Entrust on the Registration Authority (RA) function. Brian Dilley (eValid8) needed access to the RA documentation created by the Managed Service Offering (MSO) to adequately perform the audit, but the MSO has not responded favorably to his requests for that information. Although the MSO went through the 800-79 audit last year, they still do not have their audit letter. Ms. Spencer suggested that subsequent contracts say that the primary is responsible for providing the SSP with records required to remain compliant, e.g., to make these records available to the SSP for the RA.

Judith Spencer wants a cross-walk of the SSP RA requirements against the Common Policy. Jim Schminky (Treasury) funded Mr. Dilley (eValid8) to map the RA function against the Common Policy. Mr. Dilley found approximately 140 auditable events. Fifty requirements in COMMON were not addressed in NIST SP 800-79. Ms. Spencer requested that Mr. Schminky make that report available to the CPWG.

Ms. Spencer asked the FPKIPA to approve the Entrust Managed Service SSP Audit with a note stating that the RA function was not fully audited; and it voted to do so. (See the voting results table, below.)

<b>Vote to approve the Entrust Managed Service SSP Audit –without the fully audited RA function</b>			
	<b>Vote (Motion- Treasury 2<sup>nd</sup>- DoJ)</b>		
	<b>Yes</b>	<b>No</b>	<b>Abstain</b>
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)	√		
SSA	√		
USPS	√		
USPTO	ABSENT		

With respect to PIV-I, the external PKI will be responsible for the entire process. The MSO contract did not put enough emphasis on the responsibilities of the prime contractor toward the I&A for digital credentials. More emphasis was placed on the card itself. We will need recommendations to the NFI SSPs on how to address the same RA issues. We need more guidelines for PIV-I as well as for SSPs under COMMON, Ms. Spencer said.

## Agenda Item 6

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

Ms. Jenkins reported that the bandwidth project is 75% complete. There were a little over 23 Million directory hits in November. Treasury is experiencing about 245 Million internal hits per month. Some Treasury applications do real time path validation.

The FPKI MA is putting together the SOW for four sites: one for the new architecture and three for hosting repositories.

OMB has PIV-enabled the MAX website. There are plans to PIV-enable Employee Express (the on-line benefits application), as well as eTravel. Ms. Spencer recommended that CRLs get pulled down once a day, during off hours, rather than in real time, for low risk applications.

The ECC White Paper will be sent out later today, along with the FPKIA Re-Design “dashboard.”

Ms. Jenkins said the FPKI TAG is looking at improving interoperability for applications and is drafting a new white paper on how to improve path quality, which will be available in the 2<sup>nd</sup> quarter of the year.

She said the FPKI MA is in the process of letting the SOW for Audit services and hopes to get the audit letter by the end of the 2<sup>nd</sup> quarter.

## Agenda Item 7

### Adjourn Meeting

Ms. Spencer adjourned the meeting at 11:05 a.m. and the Holiday Party then began.

## 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

No.	Action Statement	POC	Start Date	Target Date	Status
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	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 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	Closed
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

No.	Action Statement	POC	Start Date	Target Date	Status
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