



**FEDERAL PKI POLICY AUTHORITY**

**March 8, 2011 MEETING MINUTES**

**USPS Headquarters  
475 L'Enfant Plaza, SW  
Conference Room: 4841  
Washington, DC  
9:35 A.M. – 10:49 A.M.**

**Welcome, Opening Remarks & Introductions**

**Deb Gallagher,  
Chair**

**Discuss / Vote on 8 February 2011 FPKIPA Minutes**

**Matt King**

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

**Charles Froehlich /  
Matt King**

- 1. Discussion: Participation in FPKI WGs**
- 2. Discussion: Charter and By-Laws Update**
- 3. Discussion: Change Proposal Compliance**
- 4. FPKI Security Profile Status**

**PIV-I Roadmap Status**

**Brant Petrick**

**FPKI Management Authority (FPKIMA) Report**

**Cheryl Jenkins /  
Wendy Brown**

- 1. SHA-256 Transition Status**

**Other Agenda Items**

**Deb Gallagher**

- *ICAM Update*
- *If you cannot attend, please designate an alternate, a proxy or an enduring proxy for such situations.*
- *Next FPKIPA meeting, 12 April 2011*

**Adjourn Meeting**

**Deb Gallagher**

## A. ATTENDANCE LIST

Voting Members:

Organization	Name	Present?
Department of Defense	Geddis, Shawn (Proxy for Debbie Mitchell)	T
Department of Energy	Breland, MaryAnn	T
Department of Health & Human Services	Slusher, Toby	P
Department of Homeland Security	Miller, Tanyette	T
Department of Justice	Morrison, Scott	P
Department of State	Frahm, Jarrod M.	P
Department of Treasury	Schminky, Jim	P
Drug Enforcement Administration (DEA CSOS)	Briggs, Sherrod (Proxy for Chris Jewell)	P
GPO	Hildebrand, Jeff (Proxy for John Hannan)	T
GSA	Gallagher, Deb	P
NASA	Levine, Susan	T
Nuclear Regulatory Commission ( NRC)	Schminky, Jim (Proxy for David Sulser)	P
SSA	Mitchell, Eric	A
USPS	Stepongzi, Mark	P
USPTO	Lindsey, Dan	A
Veterans Administration (VA)	Jurasas, Eric	T

**T – Telephone**

**P – In Person**

**A – Absent**

**B. Observers:**

Organization	Name	Present?
Cipher Solutions (Vendor)	Ahuja, Vijay	P
NASA	Baldrige, Tim	T
FPKIMA Technical Liaison (Contractor, Protiviti)	Brown, Wendy	P
eVaild8	Dilley, Brian	T
DoS (Contractor, ManTech)	Froehlich, Charles	P
USPTO (Contractor)	Jain, Amit	T
State (Contractor)	Jung, Jimmy	P
SSA	Hardy, Amy	T
FPKIPA (Protiviti)	King, Matt	P
FPKIMA (Protiviti)	Kotraba, Matt	T
DoD	Kruger, Denise	T
Noblis	Lins, Andrew	T
Entrust	Moore, Gary	P
GSA (Contractor, Unisys)	Petrick, Brant	P
EOP	Ramos, Russell "Haj"	
DHS	Shomo, Lawrence	
EPA (Contractor, Jacob & Sundstrom )	Simonetti, Dave	T
FPKIPA (Protiviti)	Sonnier, Tiffany	P
CertiPath	Spencer, Judy	P
Treasury	Wood, Daniel	P
Deloitte	Yared, Mali	T
DHS (Contractor)	Shomo, Larry	T

**T – Telephone**  
**P – In Person**  
**A – Absent**

## C. MEETING ACTIVITY

### Agenda Item 1

#### Welcome, Opening Remarks & Introductions

**Deb Gallagher, Chair**

The Federal Public Key Infrastructure Policy Authority (FPKIPA) met at the USPS Headquarters located at 475 L'Enfant Plaza, SW CR4841 Washington, DC. Ms. Deb Gallagher, Chair, called the meeting to order at 9:35 A.M. EST and introduced those present, both in person and via teleconference.

### Agenda Item 2

#### Discuss / Vote on 8 February 2011 FPKIPA Minutes

**Matt King**

Mr. King informed the FPKIPA that all corrections have been made to the circulated February 8, 2011 FPKIPA minutes. Treasury motioned to approve the minutes and the motion was seconded by HHS. The motion was approved by a 13/13 majority (100%) of members present.

Approval Vote for 8 February 2011 FPKIPA Minutes			
Voting members	Vote (Treasury Motion; HHS Second)		
	Yes	No	Abstain
Department of Defense	√		
Department of Energy	√		
Department of Health & Human Services	√		
Department of Homeland Security	√		
Department of Justice – ABSENT (for vote)			
Department of State	√		
Department of the Treasury	√		
Drug Enforcement Administration (DEA CSOS)	√		
GPO	√		
GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC) – Proxy	√		

Treasury			
SSA - ABSENT			
USPS	√		
USPTO - ABSENT			
Veterans Administration	√		

**Agenda Item 3**

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

**Charles Froehlich**

**A. Discussion: Participation in FPKI WGs**

There has been discussion about the level of participation in the CPWG by FPKIPA member agencies. It was agreed that we would institute new processes to encourage participation in the CPWG, and ensure the FPKIPA is well informed of upcoming change proposals. The process will include the following steps:

1. Initial Review: present change proposal to the CPWG.
2. FPKIPA Notification: send change proposal to the FPKIPA with a notice that it will be reviewed/finalized at the next CPWG meeting (encouraging participation).
3. Final Review: conduct final review of change proposal in the second CPWG.
4. Present to FPKIPA for Vote: send final change proposal to FPKIPA for vote at the next PA meeting

The CPWG also agreed to send CPWG Agendas to the FPKIPA to ensure members have sufficient opportunity to participate in change proposal (or other) discussions at CPWG meetings. Emergency change proposals may not follow the process above due to time constraints.

**B. Discussion: Charter and By-Laws Update**

The CPWG will be updating its Charter and Bylaws, and will keep the FPKIPA updated on its progress.

**C. Discussion: Change Proposal Compliance**

Currently, there is no verification that change proposals are adopted by cross-certified entities. Therefore, the CPWG will review the *Crits and Methods* document, looking for opportunities to establish or update enforcement mechanisms. The CPWG will update the FPKIPA on this task.

**D. FPKI Security Profile Status**

The FPKI Security Profile was presented to the ISIMC last month. The ISIMC was then given a thirty day review period. No comments have been received to-date. The next step is

to coordinate with OMB to finalize enforcement mechanism and to publish the final Profile.

#### **Agenda Item 4**

##### **PIV-I Roadmap Status**

**Brant Petrick**

The *PIV-I Certification Process Guidance* document was sent to FPKIPA mail list and will be posted to the IDManagement.gov and FPKIPA web sites. The document provides information for organizations that want to cross certify their CAs at PIV-I. This guidance is a living document and comments can be sent to Mr. Brant Petrick.

Mr. Jim Schminky summarized a CPWG discussion about a provider having an issue with customers who want PIV-I cards, but do not want to be vetted. Ms. Judy Spencer asserted that it is not a Federal PKI issue, but rather it is the provider's problem. Ms. Gallagher mentioned that this issue is being addressed by the FinC Working Group, and invited others to participate if they would like more information on this topic. Mr. Tim Baldrige mentioned that there are no enforceable regulations against making PIV-I cards look similar to PIV cards. It cannot look like a federally-supported card, but outside of that, it cannot be regulated.

#### **Agenda Item 5**

##### **FPKI Management Authority (FPKIMA) Report**

**Wendy Brown**

###### **A. SHA-256 Transition Status**

Ms. Wendy Brown provided an update on the distribution of the Common Policy Root CA certificate as part of vendor trust stores. Mozilla has accepted the application, which is now in the queue for public discussion. However, there are seventeen CA requests ahead of us.

**ACTION:** Ms. Brown will distribute the information about how to participate in the public discussion for Mozilla to the FPKIPA.

The FPKIMA requests feedback from the community regarding how long the decommissioning of Legacy CAs needs to be delayed. HHS requested a 90 day extension. No other time periods, other than DoD's request for the end of 2013, were raised.

**ACTION:** Ms. Cheryl Jenkins is scheduled to meet with the GSA DAA to request permission to keep the Legacy CAs alive past the March 31, 2011 deadline. Ms. Jenkins will notify the community of the decision.

Ms. Brown provided an update on the current status of certificates issued from the new

Infrastructure. Ms. Brown also provided highlights of the new *SHA-256 Transition Details* document, which contains a link to the certificate information created by the AIA Crawler developed in the ICAM Lab. Suggestions for better ways to depict the certificate information, are welcome. Mr. Baldrige suggested that the FPKIMA brief the Government Smart Card Interagency Advisory Board (IAB) on the AIA Crawler.

**ACTION:** The FPKIMA will brief the IAB about the AIA Crawler at the March 23, 2011 IAB meeting.

## **Agenda Item 6**

### **Other Agenda Items**

#### **ICAM Update—Ms. Gallagher**

Ms. Gallagher mentioned the FinC meeting will be held on the afternoon of 8 March 2011.

Ms. Gallagher noted that she met with DoD last week to discuss issues DoD and other agencies are experiencing related to the SHA-256 transition. A Shared Service Provider Working Group (SSPWG) meeting is scheduled for the afternoon of March 15th. SSPs are requested to provide diagrams of their infrastructures prior to the meeting. Agencies use direct trust in some cases and need this information to support the direct trust approach.

Ms. Gallagher then noted a number of upcoming meetings of interest to FPKIPA members including:

- The FPKI Technical Working Group (TWG) will be held on 17 March 2011
- The next ICAMSC meeting is 23 March 2011
- The next IAB meeting is 23 March 2011
- The ICAM Information Sharing Day is on 22 March 2011 and is open to PIV and PIV-I holders at GSA. Mr. Brant Petrick created a registration web page on [IDManagement.gov](http://IDManagement.gov) for attendees.
- The next FPKIPA meeting is 12 April 2011

## **Agenda Item 7**

### **Adjourn Meeting**

Ms. Gallagher adjourned the meeting at 10:49 AM EST.

### 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.		14-Oct-2008	12-Nov-2008	Open

No.	Action Statement	POC	Start Date	Target Date	Status
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.		9-Jun-2009	18-Jun-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.		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.		10 Nov. 2009	Oct. 2010	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
394	DOE will indicate their desire about whether to cross certify with the FBCA	Mary Ann Breland	10-Aug-2010	14-Sep-2010	Open

No.	Action Statement	POC	Start Date	Target Date	Status
	or Common				
398	Wendy Brown will send an email notifying interested parties that she will accept and respond to requests for test CA certificates with either SHA-1 or SHA-256 for testing	Wendy Brown	10-Aug-2010	14-Sep-2010	Ongoing
401	Cheryl Jenkins will draft 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
403	CPWG will draft a memo about Trusted Internet Connection (TIC) and PKIs	CPWG	14-Sep-2010	12-Oct-2010	Open
407	CPWG to discuss what changes require retesting of a PIV-I Issuer (e.g., Is retesting required if new CMS is used or other major changes are implemented?).	Matt King	14 December 2010	18 January 2011	Open
409	Matt King will add an agenda item to a future CPWG meeting related to processes for enforcing compliance with change proposals approved by the FPKIPA.	Matt King	20 January 2011	28 February 2011	Open
410	Mr. Toby Slusher agreed to send the HHS briefing on the Federal Issuers of PIV-I Cards to the FPKIPA List	Toby Slusher	20 January 2011	28 February 2011	Open

No.	Action Statement	POC	Start Date	Target Date	Status
413	Mr. King will update the SHA-256 Transition Lessons Learned document at the 15 February 2011 CPWG meeting and distribute the revised document to the SHA-256 Working Group and FPKIPA mail lists	Matt King	8 February 2011	28 February 2011	Open
414	Ms. Cheryl Jenkins will redistribute the TAG Paper on ECC to the FPKIPA Mail List	Cheryl Jenkins	8 February 2011	28 February 2011	Open
415	Ms. Gallagher will develop a plan for change management within the FPKI Community and notify the FPKIPA on how it will proceed to address change management issues such as algorithm transitions	Deb Gallagher	8 February 2011	31 March 2011	Open
416	Ms. Brown will distribute the information about how to participate in the public discussion for Mozilla to the FPKIPA	Wendy Brown	8 March 2011	15 March 2011	Closed
417	Ms. Cheryl Jenkins is scheduled to meet with the GSA DAA to request permission to keep the Legacy CAs alive past the March 31, 2011 deadline. Ms. Jenkins will notify the community of the decision.	Cheryl Jenkins	8 March 2011	15 March 2011	Closed
418	The FPKIMA will brief the IAB about the AIA Crawler at the March 23, 2011 IAB meeting.	Cheryl Jenkins	8 March 2011	23 March 2011	Closed