



FEDERAL PKI POLICY AUTHORITY

February 8, 2011 MEETING MINUTES

**USPS Headquarters
475 L'Enfant Plaza, SW
Conference Room: 4841
Washington, DC
9:35 a.m. – 11:51 a.m.**

Welcome, Opening Remarks & Introductions	Deb Gallagher, Chair
Discuss / Vote on 20 January 2011 FPKIPA Minutes	Matt King
FPKI Certificate Policy Working Group (CPWG) Report <ol style="list-style-type: none">1. CMS Requirements Change Proposal - Status2. Discuss/Vote Recommendation to Approve Verizon Business at PIV-I3. FPKI Security Controls Profile of NIST SP 800-53 and NIST SP 800-53A- Status	Charles Froehlich
FPKI Management Authority (FPKI MA) Report	Cheryl Jenkins
SHA-256 Transition <ol style="list-style-type: none">1. Lessons Learned2. DoD / VA Update3. FPKIPA External Relationships and Requirement Impacts	All
Other Agenda Items <ol style="list-style-type: none">1. ICAM Update—Deb Gallagher2. If you cannot attend, please designate a proxy3. Next FPKIPA meeting, 8 March 2011	Deb Gallagher
Adjourn Meeting	Deb Gallagher

A. ATTENDANCE LIST

Voting Members:

Organization	Name	Present?
Department of Defense	Mitchell, Debbie	P
Department of Energy	Breland, MaryAnn	T
Department of Health & Human Services	Slusher, Toby	P
Department of Homeland Security	Miller, Tanyette (Proxy for Don Hagerling)	P
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)	T
GPO	Hildebrand, Jeff (Proxy for John Hannan)	T
GSA	Gallagher, Deb	P
NASA	Morris, Justin (Proxy for Susan Levine)	T
Nuclear Regulatory Commission (NRC)	Sulser, David	P
SSA	Mitchell, Eric	T
USPS	Stepongzi, Mark	P
USPTO	Lindsey, Dan	T
Veterans Administration (VA)	Jurasas, Eric	P

T – Telephone

P – In Person

A – Absent

B. Observers:

Organization	Name	Present?
NASA	Baldrige, Tim	T
Treasury	Bracy, Gayle	T
FPKI MA Technical Liaison (Contractor, Protiviti)	Brown, Wendy	P
DoD (Contractor, Booz Allen)	Frank, Larry	T
DoS (Contractor, ManTech)	Froehlich, Charles	P
USPTO (Contractor)	Jain, Amit	T
GSA, FPKI MA PM	Jenkins, Cheryl	T
State (Contractor)	Jung, Jimmy	P
FPKIPA (Protiviti)	King, Matt	P
DoD	Kruger, Denise	T
Noblis	Lins, Andrew	T
FPKIPA (Protiviti)	Louden, Chris	P
VA	Miller, Jason	P
Entrust	Moore, Gary	P
GSA (Contractor, Unisys)	Petrick, Brant	P
DoD	Ryan, George	T
DISA	Scogin, Allison	P
EPA (Contractor, Jacob & Sundstrom)	Simonetti, Dave	T
FPKIPA (Protiviti)	Sonnier, Tiffany	P
CMS	Huza, Chris	T
CertiPath	Spencer, Judy	P
DoD (Contractor)	Wallace, Carl	P
Verizon Business	Weiser, Russ	P
DHS (Contractor)	Shomo, Larry	T
	Hardy, Amy	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. 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 20 January 2011 FPKIPA Minutes

Matt King

Mr. King informed the FPKIPA that some additional, minor, editorial corrections were made to the January 20, 2011 FPKIPA minutes circulated prior to the meeting. Treasury motioned to approve the minutes and the motion was seconded by State. The motion was approved by a 16/16 majority (100%)

Approval Vote for 20 January 2011 FPKIPA Minutes			
Voting members	Vote (Motion Treasury ; 2 nd 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 3

FPKI Certificate Policy Working Group (CPWG) Report

Charles Froehlich

CMS Requirements Change Proposal - Status

The status of a change proposal resulting from discussions with CertiPath was provided. The content of the change proposal was agreed to in the last CPWG meeting and the formal review of the change proposal will be held at the 15 February CPWG meeting. This change proposal will simply clarify that the rules for role separation also apply to the Card Management System (CMS).

ACTION: Mr. King agreed to send the new change proposal, *CMS Requirements Clarification*, for an E-Vote after the change proposal is agreed upon by the CPWG (expected by 15 or 16 February 2011).

Discuss/Vote Recommendation to Approve Verizon Business at PIV-I

Verizon Business has passed PIV-I testing and completed all steps to become an Approved PIV-I provider. The CPWG recommended that they be approved for PIV-I cross certification. Treasury motioned to approve Verizon at PIV-I and the motion was seconded by USPS. The motion was approved by a 15/16 majority (93.8%).

Approval Vote for Verizon Business at PIV-I			
Voting members	Vote (Motion Treasury; 2 nd USPS)		
	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 (Proxy to GSA)	√		
Drug Enforcement Administration (DEA CSOS)	√		
GPO	√		

GSA	√		
NASA	√		
Nuclear Regulatory Commission (NRC)	√		
SSA	√		
USPS	√		
USPTO	√		
Veterans Administration	√		

FPKI Security Controls Profiles of NIST SP 800-53 and NIST SP 800-53A – Status

The FPKI Security Controls Profiles have been finalized and all format changes recommended by NIST have been incorporated. Ms. Gallagher will brief the ISIMC on 9 February 2011. After the ISIMC briefing, Ms. Gallagher will work with OMB to identify the appropriate enforcement mechanism that will require compliance with the profiles. Ms. Gallagher mentioned that the ISIMC is also reviewing NIST SP 800-53 and expects the profile will be well-received.

Agenda Item 4

FPKI Management Authority (FPKI MA) Report

Wendy Brown

The FPKI ATO letter has been posted to the FPKI MA web site. The cross-certificates from the Legacy Common Policy CA to the SHA-1 FRCA and to the new Common Policy CA have been issued. Progress has been made in getting the Common Policy CA certificate into various Trust Stores. The certificate is expected to be available via the Microsoft root update package by March 22, 2011. Applications to add the Common Policy CA certificate to the Adobe, Mozilla, and Apple Trust Stores have been submitted, but no firm dates for distribution have been provided. Cross-certificates continue to be issued to partners. All cross-certificates will be issued by the 31 March 2011 deadline.

Agenda Item 5
SHA-256 Transition
Deb Gallagher

Ms. Gallagher opened the discussion with mention of OMB Memo M-11-11. Ms. Gallagher explained that the memo outlines a plan of action that will expedite the full use of PIV credentials for access to Federal facilities and information systems. The memo is intended to bring forces together to gain efficiencies and help understand what is going on across the Government regarding PIV credential use and implementation. Ms. Gallagher noted that the fourth bullet on page four of the memo, which requires electronic verification of PIV credentials, significantly impacts the FPKI community.

ACTION: Mr. Brant Petrick will post OMB Memo M-11-11 to the IDManagement.gov web site.

Lessons Learned

Discussion of the lessons learned from the SHA-256 Transition was held. Mr. King captured the results of the discussion in a document that includes four categories of lessons learned: Technical Support, Communications, Timing, and Planning. The document will be discussed further at the 15 February 2011 CPWG meeting, updated, and distributed to the SHA-256 Working Group and FPKIPA mail lists.

ACTION: 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.

ACTION: Ms. Cheryl Jenkins will redistribute the TAG Paper on ECC to the FPKIPA Mail List.

ACTION: 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.

DoD / VA Update

Ms. Allison Scogin presented a briefing on the status of the DoD/VA issue. The briefing described the current and potential future states of the certificate path validation for VA credentials and identified the causes of current issues, and issues that may arise in the future when the FPKIPA sunsets the Legacy infrastructure. One main concern raised is whether applications will be able to process multiple validation paths.

The main problem was summarized as follows: "When Verizon Business Betrustrated Production SSP CA A1 subordinates to the Federal Common Policy CA on 03/31/2011,

legacy Navy systems will NO LONGER be able to validate the SHA 1 VA PKI PIV certificates issued prior to 12/31/2010.” Further discussion was held and a potential “FPKI-approved” solution is available: issuance of a cross-certificate from the SHA-1 FRCA to the Verizon Business CA.

The FPKI MA and DoD/VA agreed that they would coordinate further on the potential solution in a meeting on 9 February 2011.

FPKIPA External Relationships and Requirement Impacts

It was agreed that any plan for change management (mentioned above in the Lessons Learned section) would need to include management of external relationships and impact of external requirements.

Agenda Item 6

Other Agenda Items

ICAM Update—Ms. Gallagher

1. The next ICAMSC Meeting is 23 February 2011.
2. The Next FPKIPA meeting is 8 March 2011.

Agenda Item 7

Adjourn Meeting

Ms. Gallagher adjourned the meeting at 11:51 a.m. 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
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

No.	Action Statement	POC	Start Date	Target Date	Status
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
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
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

No.	Action Statement	POC	Start Date	Target Date	Status
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	Closed
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
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
411	Mr. Matt King agreed to send the new change proposal, "CMS Requirements Clarification," for an E-Vote after the change proposal is approved by the CPWG (expected by 15 or 16	Matt King	8 February 2011	16 February 2011	Closed

No.	Action Statement	POC	Start Date	Target Date	Status
	February).				
412	Mr. Brant Petrick will post OMB Memo 11-11 to the IDManagement.gov web site	Brant Petrick	8 February 2011	16 February 2011	Closed
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