



FEDERAL PKI POLICY AUTHORITY

May 10, 2011 MEETING MINUTES

**USPS Headquarters
475 L'Enfant Plaza, SW
Conference Room: 4841
Washington, DC
9:31 a.m. – 10:34 a.m.**

Welcome, Opening Remarks & Introductions	Deb Gallagher, Chair
Discuss / Vote on April 12, 2011 FPKIPA Minutes	Matt King
FPKI Certificate Policy Working Group (CPWG) Report <ul style="list-style-type: none">• FIPS 201-2 Review and Comment – Status• SHA-256 Lessons Learned Document - Status	Charles Froehlich
FPKI Management Authority (FPKIMA) Report	Cheryl Jenkins
Other Agenda Items <ul style="list-style-type: none">• ICAM Update• Next FPKIPA meeting: June 14, 2011	Deb Gallagher
Adjourn Meeting	Deb Gallagher

A. ATTENDANCE LIST

a. Voting Members

Organization	Name	T – Telephone P – In Person A – Absent
Department of Defense (DoD)	Mitchell, Debbie	T
Department of Energy (DOE)	Breland, MaryAnn	A
Department of Health & Human Services (HHS)	Slusher, Toby	P
Department of Homeland Security (DHS)	Miller, Tanyette (Proxy for Don Hagerling)	A
Department of Justice (DOJ)	Morrison, Scott	P
Department of State (State)	Frahm, Jarrod M.	P
Department of Treasury (Treasury)	Schminky, Jim	P
Drug Enforcement Administration (DEA CSOS)	Briggs, Sherrod (Proxy for Chris Jewell)	T
Government Printing Office (GPO)	Hannan, John	T
General Services Administration (GSA)	Gallagher, Deb	P
National Aeronautics & Space Administration (NASA)	Levine, Susan	T
Nuclear Regulatory Commission (NRC)	Sulser, David	P
Social Security Administration (SSA)	Mitchell, Eric	T
United States Postal Service (USPS)	Stepongzi, Mark	P
United States Patent & Trademark Office (USPTO)	Lindsey, Dan	T
Veterans Administration (VA)	Jurasas, Eric	T

b. Observers

Organization	Name	T – Telephone P – In Person
CertiPath	Spencer, Judy	P
DoD	Kruger, Denise	T
DoD (Contractor, Booz Allen)	Frank, Larry	T
DoS (Contractor, ManTech)	Froehlich, Charles	P
Entrust	Moore, Gary	P
FPKIMA Technical Liaison (Contractor, Protiviti)	Brown, Wendy	P
FPKIPA (Contractor, Protiviti)	King, Matt	P
FPKIPA (Contractor, Protiviti)	Sonnier, Tiffany	P
GSA (Contractor, Unisys)	Petrick, Brant	P
GSA, FPKIMA PM	Jenkins, Cheryl	P
NASA	Baldrige, Tim	T
State (Contractor)	Jung, Jimmy	T
USPTO (Contractor)	Jain, Amit	T
DoD (Contractor, Booz Allen)	Jeffers, Dan	T
FPKIMA (Contractor, Protiviti)	Jarboe, Jeff	P
State of Illinois	Wells, Gordon	T
DHS	Shomo, Larry	T
US Access	Smith, Jackie	T
EOP	Ramos, Russell "Haj"	T

B. MEETING ACTIVITY

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 9:31 a.m. EST and introduced those present, both in person and via teleconference.

Discuss / Vote on April 12, 2011 FPKIPA Minutes, Matt King

There was a vote to approve the April 12, 2011 FPKIPA minutes. The State Department motioned to approve; USPS seconded. The motion was approved unanimously.

Approval Vote for April 12, 2011 FPKIPA Minutes			
Voting members	Vote (State Motion; USPS 2nd)		
	Yes	No	Abstain
Department of Defense (DOD)	√		
Department of Energy (DOE)	Absent		
Department of Health & Human Services (HHS)	√		
Department of Homeland Security (DHS)	Absent		
Department of Justice (DOJ)	√		
Department of State (State)	√		
Department of the Treasury (Treasury)	√		
Drug Enforcement Administration (DEA CSOS)	√		
Government Printing Office (GPO)	√		
General Services Administration (GSA)	√		
National Aeronautics & Space Administration (NASA)	√		
Nuclear Regulatory Commission (NRC)	√		
Social Security Administration (SSA)	√		
United States Postal Service (USPS)	√		
United States Patent & Trademark Office (USPTO)	√		
Veterans Administration (VA)	√		

FPKI Certificate Policy Working Group (CPWG) Report, Charles Froehlich

Mr. Charles Froehlich mentioned that there will be no discussion or vote on the Common Policy Device Certificate Validation Clarification Change Proposal or the PIV-I Issuer Retesting Requirements because these items were not discussed at the last CPWG meeting. Mr. Froehlich proceeded to provide status on the following:

FIPS 201-2 Review and Comment – Status

The CPWG had a lengthy discussion of the FIPS 201-2 comments, and that the CPWG was able to get through 2/3 of the comments submitted by the AWG and CPWG. Mr. Froehlich noted the AWG will host a joint AWG/CPWG Meeting on May 11th to finalize the review of the comments.

SHA-256 Lessons Learned Document – Status

The CPWG was able to complete a partial review of the Lessons Learned document. The document is expected to be finalized at the next CPWG (May 17, 2011).

FPKI Management Authority (FPKIMA) Report, Cheryl Jenkins

Ms. Wendy Brown stated that during public discussion related to the submission of the Common Policy CA root certificate to Mozilla, the CA/Browser (CAB) Forum Base Requirements document was brought to the attention of the FPKIMA. The document defines the base requirements for a CA to be trusted for inclusion in relying party application trust stores. CAB Forum relying party members include Apple, Google, KDE, Microsoft, Opera, Rim, and Mozilla. Many commercial FPKI Affiliates are CA members of the CAB Forum.

The FPKIMA will do a GAP analysis of the CAB Forum Base Requirements against the FPKI Certificate Policies, and will provide comments and recommendations. The FPKIMA will present their analysis and recommendations for review at the next CPWG meeting (May 17, 2011). The CAB Forum and its Base Requirements document are important because of their implications. If the Base Requirements document is accepted by the various CAB Forum members, it may mean that a CA (like the Common Policy CA) only has to apply once to be included in all browser trust stores, rather than submitting multiple applications.

It was also noted that this is an opportunity to provide feedback on ways to improve the CAB Forum Base Requirements document, and to gain insight about the current practices of commercial CAs that are members of the CAB Forum, which may be used to improve the FPKI Certificate Policies.

Ms. Cheryl Jenkins then displayed the current status of certificate management for the transition. Illinois is the only CA that still has only a cross-certificate to the legacy

FBCA. Illinois is planning to move to the SHA1 FRCA before the end of May. Ms Jenkins noted that about 42% of the legacy cross-certificates have expired or have been revoked to-date. Ms. Jenkins requested that all Affiliates complete their testing of the new certificate paths, and let the FPKIMA know when they are ready for the legacy certificates to be revoked.

Ms. Jenkins informed the FPKIPA that she has been working with the DAA to ensure that the legacy CAs can continue to operate until all Affiliates have completed the transition to the new Trust Infrastructure. Ms. Jenkins has just completed a scan showing the vulnerabilities so the DAA can accept the risks identified allowing the FPKIMA to continue operating the old systems. Ms. Jenkins stated that the risks are low, but the FPKIMA wants to finish sun-setting these systems by June 30, 2011.

Mr. Toby Slusher asked if the ultimate sunset date is June 30, 2011. Ms. Jenkins responded yes.

Ms. Susan Levine and Mr. Tim Baldrige stated that they had initially asked for a late May 2011 date for revocation of the Treasury and Treasury SSP certificates, but because of a delay in NASA shuttle flights, they would now prefer that their certificates be revoked today or tomorrow. Ms. Jenkins said she would try to get the FPKIMA to find the resources to cooperate with this request.

Ms. Debbie Mitchell stated that Mr. Dan Jeffers is still looking for root certificates required for configuring systems that rely on direct trust. Ms. Brown replied that she believes they are all available on the AIA web crawler output, but if Mr. Jeffers would supply a list of what certificates he feels are missing, the FPKIMA will help get copies of the missing certificates. Not everyone has responded to the request to supply their root certificate along with sample end-entity certificates.

Mr. Scott Morrison asked if all the legacy certificates had been removed from the repositories as was discussed at the last FPKIPA meeting. Ms. Jenkins and Ms. Brown responded that the legacy certificates were removed from the FPKI repositories on April 27, 2011 with the exception of Illinois, which does not have a new path yet. However, not all Affiliates have removed all the legacy certificates from their own repositories. Therefore, there is still the possibility that an old SHA1 path will be found during certificate validation.

Ms. Jenkins then presented additional projects the FPKIMA is initiating, including improving the capacity and security posture of the FPKI by reviewing the protocol requirements for repositories. This will be a topic at the upcoming FPKI TWG.

The FPKIMA is looking at improving communications and problem resolution with the FPKI community, and will be setting up a knowledge base and automated reporting. These improvements are expected to provide a better way of communicating information from the monthly statistical report.

Based on lessons learned from the transition to SHA-256, the FPKI TWG has been tasked with developing better ways of communicating upcoming transitions to the community, including developing a transition framework. Mr. Jim Schminky mentioned that the GSA MSO has developed a transition framework and the FPKIMA should look at that for input.

Other Agenda Items

ICAM Update, Deb Gallagher

Ms. Gallagher invited the FPKIPA to the next ICAM Subcommittee (ICAMSC) meeting (Wednesday, May 18, 2011). The ICAMSC meeting agenda includes identity management training conducted by the Smart Card Alliance Group, and discussion of the Federated PACS Guidance document. Ms Gallagher stated comments on the PACS guidance are due by Friday May 13. If FPKIPA members are interested in attending the upcoming ICAMSC meeting, let Ms. Gallagher know.

Ms Gallagher mentioned there is a growing interest in the Trust Framework Adoption Process and that SAFE BioPharma has indicated an interest because it would allow them to leverage their lower assurance level certificates (currently approved at basic and medium levels of assurance) as an identity provider and a trust framework provider.

Digital signature guidance is still in OMB internal review. Through the ICAMSC, the Electronic Signature guidance has been developed. Community members who have seen the guidance are in favor of it, but the guidance is still going through coordination and is not ready to be distributed to the entire ICAMSC. The document describes when an electronic signature can be used and provides guidance.

Ms. Gallagher informed the FPKIPA that the FPKI Security Profile was accepted for inclusion in FISMA and posted to the FPKIPA website; OMB has accepted the FPKI Security Profile.

Ms. Jenkins stated that the Continuous Monitoring Framework is now part of FISMA and is a part of the required reporting. Reviewers of FISMA reporting may have questions and will want to ensure that if someone is a PKI provider, they should be following the FPKI Security Profile. The FPKIMA would like to be able give assurance that by following the FPKI Security Profile, a PKI provider is in compliance with FISMA requirements.

Mr. King suggested that it be would be a good idea for the FPKIPA Chair to issue a memo that explains how Government-operated PKIs are required to follow the FPKI Security Profile for the new FISMA reporting metrics. A memo would provide an authoritative source for PKI providers to provide to the agency DAAs. Ms Gallagher stated she needs to explore this option soon.

ACTION: Matt King will work with Deb Gallagher to draft a memo that explains how Government-operated PKIs are required to follow the FPKI Security Profile for the new FISMA reporting metrics

- The next ICAMSC meeting is May 18, 2011
- The next Government Smart Card Interagency Advisory Board (IAB) meeting is May 18, 2011
- The next FPKIPA meeting is June 14, 2011

Adjourn Meeting

Ms. Gallagher adjourned the FPKIPA meeting at 10:34 a.m. EST.

FPKIPA 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 Ms. Jenkins will follow up to make sure the test plan includes testing at the application level,--not just the PKI level.	Debbie Mitchell, FPKIPA, Ms. 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	Ms. Jenkins will send out guidance to the agencies on how to use the various root stores.	Ms. Jenkins	9 Jun 2009	14 Jul 2009	Open

No.	Action Statement	POC	Start Date	Target Date	Status
379	Ms. 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.	Ms. 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	Ms. 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.	Ms. Brown	10 Nov 2009	16 Nov 2009	Open
385	We need to write a Change Proposal, adding a cardAuth policy to FBCA. FBCA will require a UUID, as opposed to being optional.		10 Nov 2009	30 Nov 2009	Obsolete by PIV-I
386	Mr. Jim Schminky will provide the FPKIMA with a report of availability from a	Jim Schminky	10 Nov 2009	30 Nov 2009	Obsolete

No.	Action Statement	POC	Start Date	Target Date	Status
	customer point of view, since Treasury does its own monitoring of availability of the FPKIA repositories.				
388	Ms. 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.	Ms. Jenkins	9 Mar 2010	13 Apr 2010	Open
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	Closed – by default they stayed with FBCA since they did not request a move
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
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		10 Aug 2010	14 Sep 2010	Closed
398	Ms. 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	Ms. Brown	10 Aug 2010	14 Sep 2010	Ongoing

No.	Action Statement	POC	Start Date	Target Date	Status
401	Ms. 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	Ms. 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
404	Matt King will write a SHA-256 FAQ and distribute it on or about 1 December	Matt King	9 Nov 2010	1 Dec 2010	Closed
406	Ms. Jenkins will provide guidance on how to transition to the new SHA-256 FPKI	Ms. Jenkins	9 Nov 2010	1 Dec 2010	Closed
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 Dec 2010	18 Jan 2011	Open
408	Once Verizon Business PIV-I testing is complete, an email vote will be held to approve Verizon Business at PIV-I	Matt King	14 Dec 2010	18 Jan 2011	Closed
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 Jan 2011	28 Jan 2011	Open

No.	Action Statement	POC	Start Date	Target Date	Status
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 Jan 2011	28 Feb 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 February).	Matt King	8 Feb 2011	16 Feb 2011	Closed
412	Mr. Brant Petrick will post OMB Memo 11-11 to the IDManagement.gov web site	Brant Petrick	8 Feb 2011	16 Feb 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 Feb 2011	28 Feb 2011	Open
414	Ms. Ms. Jenkins will redistribute the TAG Paper on ECC to the FPKIPA Mail List	Ms. Jenkins	8 Feb 2011	28 Feb 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 Feb 2011	31 Mar 2011	Open

No.	Action Statement	POC	Start Date	Target Date	Status
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
419	Ms. Wendy Brown will submit proposed language from the Device Certificates Validation Clarification change proposal to the Mozilla public discussion to see if the change would satisfy their concern.	Wendy Brown	12 April 2011	29 April 2011	Open
420	The FPKIMA will resend the request for Affiliates to test and notify the FPKIMA when legacy certificates can be revoked, but this time includes a request to remove the legacy certificates from public repositories.	Wendy Brown	12 April 2011	15 April 2011	Closed
421	The request to send sample end-entity certificates for testing should also be resent, this time with a request a request that Root certificates be included.	Wendy Brown	12 April 2011	15 April 2011	Closed

No.	Action Statement	POC	Start Date	Target Date	Status
422	Any agency that would like their cross certificates removed from the FPKI repository before April 27th will notify the FPKIMA.	All Affiliates	12 April 2011	27 April 2011	Open
423	Ms. Wendy Brown will send a notice to agencies informing them that all certificates will be removed from the FPKI repositories by April 27th and that all legacy cross certificates should be revoked no later than May 25, 2011.	Wendy Brown	12 April 2011	15 April 2011	Closed
424	Matt King will work with Deb Gallagher to draft a memo that explains how Government-operated PKIs are required to follow the FPKI Security Profile by the new FISMA reporting metrics.	Matt King	May 10, 2011	June 2, 2011	Open