



FEDERAL PKI POLICY AUTHORITY

June 14, 2011 MEETING MINUTES

**USPS Headquarters
475 L'Enfant Plaza, SW
Conference Room: 4841
Washington, DC
9:35 a.m. – 11:08 a.m.**

Welcome, Opening Remarks & Introductions	Deb Gallagher, Chair
Discuss / Vote on May 10, 2011 FPKIPA Minutes	Matt King
FPKI Certificate Policy Working Group (CPWG) Report	Matt King
FPKI Management Authority (FPKIMA) Report	Cheryl Jenkins
FPKI Security Profile Memo (FISMA Reporting Metrics)	Deb Gallagher
Other Agenda Items <ul style="list-style-type: none">○ <i>ICAM Update—Deb Gallagher</i>○ <i>If you cannot attend, please designate an alternate, a proxy or an enduring proxy for such situations.</i>○ <i>Next FPKIPA meeting is July 12, 2011</i>	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)	P
Department of Justice (DOJ)	Morrison, Scott	P
Department of State (State)	Frahm, Jarrod M.	T
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 (Proxy to GSA)	T
General Services Administration (GSA)	Gallagher, Deb	P
National Aeronautics & Space Administration (NASA)	Wyatt, Terry	T
Nuclear Regulatory Commission (NRC)	Sulser, David	P
Social Security Administration (SSA)	Mitchell, Eric	A
United States Postal Service (USPS)	Stepongzi, Mark	P
United States Patent & Trademark Office (USPTO)	Lindsey, Dan (Proxy to GSA)	A
Veterans Administration (VA)	Jurasas, Eric	A

b. Observers

Organization	Name	T – Telephone P – In Person
CertiPath	Spencer, Judy	P
DoD (Contractor, Booz Allen)	Frank, Larry	T
E-Valid8	Brian Dilley	P
Entrust	Moore, Gary	T
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
NASA	Baldrige, Tim	T
FPKIMA (Contractor)	Louden, Chris	P
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	Schomo, Larry	T
EPA (Contractor, Jacob & Sundstrom)	Simonetti, Dave	T
Safer Institute	Boley, Ken	P

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 9:35 a.m. EST and those present, both in person and via teleconference, introduced themselves.

Discuss / Vote on May 10, 2011 FPKIPA Minutes, Matt King

There was a vote to approve the May 10, 2011 FPKIPA minutes. HHS motioned to approve; NRC seconded. The motion was approved unanimously.

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

FPKI Certificate Policy Working Group (CPWG) Report, Matt King

The change proposal to Common Policy clarifying requirements for device certificates will not be voted on today due to additional comments being received as well as ongoing discussions with the CAB Forum. The change proposal was to clarify the need to verify the subject of a device certificate and to ensure it is in control of the human sponsor. The CPWG does not want to go forward with the change proposal until the CPWG hears if there are additional concerns from the CAB Forum and Mozilla.

The next CPWG will discuss PIV-I retesting requirements, and may discuss the C4CA change proposal introduced by Mr. Scott Rea.

Mr. Toby Slusher stated that HHS is still looking at the requirement and would not be ready to provide use cases by next week's CPWG. Mr. King said he has not sent a request to FPKIPA members asking if any agency wanted to sponsor the change proposal yet, as he had been waiting for an updated change proposal from Mr. Rea.

Mr. Chris Loudon and Ms. Debbie Mitchell asked if there is a reason to keep the C4CA active. They added that no one currently uses the C4CA.

C4CA was originally established for PKIs that were not at the bridge level. Mr. Loudon suggested that all the historical reasons for adding C4CA have been overtaken by events. Ms. Brown informed FPKIPA members that DigiCert was asked to obtain a federal sponsor for the C4CA change proposal and the CPWG decided to defer discussion until a federal sponsor for the change proposal is found. HHS will take a look at whether there is a legitimate business need for the C4CA. HHS will complete its review and provide the CPWG with either use cases or an update that HHS no longer needs C4CA.

It was requested that Mr. King send a request to the FPKIPA members to see if there was still a requirement from any agency for the C4CA, or if all requirements could be met by the FBCA.

ACTION: Mr. King will send a request to the FPKIPA members to see if there was still a requirement from any agency for the C4CA, or if all requirements could be met by the FBCA.

FPKI Management Authority (FPKIMA) Report, Cheryl Jenkins

Mr. Jeff Jarboe presented the FPKIMA report on behalf of Ms. Cheryl Jenkins.

SHA-2- Mr. Jarboe reported 97% of the required new certificates have been issued and 88% of the old certificates have been revoked or expired. The remaining certificate to be issued in order to complete the migration to the new CAs belongs to Illinois.

The only change from last month to this month was receiving information from Opera that they did receive the FPKIMA's application to be added to their browser trust store.

The DAA has given temporary approval to operate legacy CAs until June 30, 2011 which aligns with the plan to decommission the legacy CAs by June 30. To date, there are only six cross certificates left to revoke. The revocation of these certificates has been delayed until June 28th, 2011. Mr. Louden cautioned meeting participants that no further extension has been given and it would take more than the FPKIPA to change the deadline so agencies need to be aware of the approaching deadline. Mr. Louden added that a number of agencies have asked that the legacy certificates stay in place until the 28th. Ms. Deb Gallagher encouraged agencies to be proactive in providing permission to the FPKIMA to revoke their legacy cross certificates.

FPKIMA Initiatives- In support of an effort to provide E-Governance Trust Services (EGTS) to the Federal Government, the FPKIMA plans to repurpose one of the EGCA's, which was established for Level 1 Credential Service Providers, but never used. This repurposed CA will support EGTS services.

The EGCA CP has been revised to establish several new certificate policies that will be required for E-Governance Trust Services such as Backend Attribute Exchange (BAE) and metadata services. The first certificate policy that will be supported is for BAE Brokers. Mr. Chris Louden explained one of the scenarios for these new certificate policies.

CAB Forum baseline requirement- The FPKIMA conducted a gap analysis to compare CAB Forum baseline requirements to FPKI policies and discussed the list of comments at the last CPWG. A final list of comments was sent to the Certificate Authority Browser (CAB) forum. The forum is a collection of certificate vendors who set best practices and guidelines for how CAs are included in Browser trust stores. The gap analysis identified three areas for changes to the Common Policy Certificate profile for device certificates. The FPKIMA will be providing a change proposal to address these changes in the device certificate profile to the CPWG at a later time.

FPKI TWG Updates- The FPKI TWG is this Thursday at NOMA in room 801 from 9:30 am to 3:30 pm. A discussion of the community interoperability test environment will be discussed.

Microsoft will be at the TWG to discuss what their requirements for a time-stamp service are and what impact it has for inclusion of the Common Policy CA root certificate in their trust store. Alternatives to the time-stamping requirement will also be discussed. Ms. Deb Gallagher wants a thorough analysis to be done. The analysis Ms. Gallagher is looking for is whether or not there is a requirement to do time-stamping and if so what are the requirements, and why are they needed. Ms. Wendy Brown urged anyone who is using code signing to participate since the scope of the meeting is to understand

Microsoft's requirement and its impacts on CAs that issue code signing certificates. Ms. Gallagher suggested that options may need to be discussed as time stamping services can be very expensive. Ms. Judy Spencer added that if Microsoft could explain their requirements, then agencies can suggest counterpoints. Mr. Chris Loudon stated that the TWG has sent questions to Microsoft and their replies have been sent out to the group.

Ms. Brown and Mr. Jarboe stated a recommendation to eliminate the requirement for LDAP support in FPKI repositories will be discussed at the TWG, but noted it will require changes to the CPs, and certificate profiles.

In response to lessons learned from the SHA 2 transition and the need for better coordination, the FPKIMA is recommending a strategy for versioning and updates for support of new capabilities to prepare for major changes in the trust infrastructure.

Mr. Tim Baldrige noted that there are a significant number of entities that depend on the FPKI that are still unaware of the changes that have taken place. For example, he noted that there have been problems related to deprecation of the 1024-bit key resulting in invalid policy mapping. Mr. Baldrige suggested that marketing is needed to communicate changes and to be proactive for future changes, beginning now with the move to Elliptic Curve Cryptography (ECC).

Regarding the move to ECC, no date has been decided but has to be made soon; discussions with NIST regarding the move to ECC have already begun. One lesson learned from the SHA 2 transition, is that there was no testing environment. The FPKIMA will be supporting the FPKIMA Certificate Authorities and affiliates with a test environment. An FPKI Community Interoperability Test Environment will be discussed at the upcoming TWG.

FPKI Security Profile Memo (FISMA Reporting Metrics), Deb Gallagher

Ms. Gallagher submitted the FPKI Security Profile for inclusion in the latest FISMA metrics, but the Profile was not included this time since more direction was needed about what to include. Ms. Gallagher and Mr. Matt King will have a meeting to get the FPKI security profile into the FISMA reporting metrics for September. Ms. Gallagher also mentioned that Cyberscope, the application used for reporting FISMA metrics, is PIV-enabled. They released the last set of metrics in the last quarter and would like for it to go in the annual metrics due in September. FISMA reporting is a requirement for Federal agencies.

Other Agenda Items, Deb Gallagher

ICAM Update

The next ICAM Subcommittee (SC) meeting is June 29 from 10:00 a.m. to 12:00 p.m. The Government Smart Card Interagency Advisory Board (IAB) meeting is also June 29 from 1:00 p.m. to 4:00 p.m. Ms. Gallagher mentioned that since NSTIC launched in mid April, three workshops have been set up to help get questions answered and to develop a steering body. The next workshop will be held at the end of June and focus on privacy and the final workshop will be held in September and focus on standards.

Ms. Gallagher also mentioned an OMB memo that will be released soon requiring Federal agency applications to accept third party credentials (Levels 1, 2, and non-PKI Level 3) via federal government websites. Ms. Gallagher noted that a revision to NIST SP 800-63 will be released soon for comment and she will notify the FPKIPA when the comment period starts.

Chapters 7, 8, and 12 of the FICAM Roadmap are being finalized for release and public comment/review. The digital signature guidance was released by OMB and forwarded to the ICAMSC for comments. So far, no comments have been received.

The next FPKIPA meeting is July 12 at the United States Postal Service Headquarters.

ACTION: Ms. Deb Gallagher agreed to send the digital signature guidance to the Federal members of the FPKIPA.

The next ICAMSC meeting is June 29, 2011.

The next Government Smart Card IAB meeting is June 29, 2011.

The next FPKIPA meeting is July 12, 2011.

Adjourn Meeting

Ms. Gallagher adjourned the FPKIPA meeting at 11:08 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	Ms. Jenkins	9 Jun 2009	14 Jul 2009	Open

No.	Action Statement	POC	Start Date	Target Date	Status
	root stores.				
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		10 Nov 2009	30 Nov 2009	Obsolete by PIV-I

No.	Action Statement	POC	Start Date	Target Date	Status
	being optional.				
386	Mr. Jim Schminky will provide the FPKIMA 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	Obsolete
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	Ms. Brown	10 Aug 2010	14 Sep 2010	Ongoing

No.	Action Statement	POC	Start Date	Target Date	Status
	for testing				
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	Matt King	20 Jan 2011	28 Jan 2011	Open

No.	Action Statement	POC	Start Date	Target Date	Status
	proposals approved by the FPKIPA.				
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	Deb Gallagher	8 Feb 2011	31 Mar 2011	Open

No.	Action Statement	POC	Start Date	Target Date	Status
	notify the FPKIPA on how it will proceed to address change management issues such as algorithm transitions				
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	Mr. Jim Schminky will draft a change proposal to generate a live test card in a production environment. After generating the change proposal, FIPS 201 may need to be updated.	Jim Schminky	April 12, 2011	May 10, 2011	Open
420	Mr. Matt King will submit a request for comments to be received by next CPWG meeting on May 5 th .	Matt King	April 12, 2011	May 5, 2011	Closed
421	Mr. King will distribute the document as- is and add comments, implementation and enforcement to the next agenda.	Matt King	April 12, 2011	May 10, 2011	Closed

No.	Action Statement	POC	Start Date	Target Date	Status
422	Mr. King will circulate proposed change proposal to the Policy Authority (PA) for review with the comment that members of the PA are encourage to attend May 5ths CPWG meeting if there are any concerns and they will be discussed during the meeting.	Matt King	April 12, 2011	May 5, 2011	Open
423	If no concerns the change proposal will be presented for vote at the May 10 th PA meeting.	Matt King	April 12, 2011	May 10, 2011	Open
424	DOE will put what they heard in document form and send to the CPWG for confirmation, and will then re-submit their application based on the advice given	Mary Ann Breland	April 12, 2011	May 10, 2011	Open
425	Mr. King will coordinate with Mr. Baldrige and Mr. Dave Silver to request comments on FIPS 201-2 from both the AWG and CPWG, and to invite the AWG to the CPWG on the morning of 5 May to discuss FIPS 201-2 comments	Matt King, Tim Baldrige	April 12, 2011	May 5, 2011	Closed
426	Ms. Deb Gallagher will send comments regarding FIPS 201-2 that are gathered at the May 5 th joint CPWG/AWG meeting to ICAMSC	Deb Gallagher	April 12, 2011	June 2, 2011	Open
427	Mr. King will cancel the April 19 CPWG meeting, and move the SHA-256 meeting to May 5th	Matt King	April 12, 2011	April 19, 2011	Closed

No.	Action Statement	POC	Start Date	Target Date	Status
428	After the joint CPWG/AWG meeting, the FIPS 201-2 document will be submitted to FPKIPA on the 10 th of May.	Matt King	April 12, 2011	May 10, 2011	Open
429	<p>Mr. Matt King will ask ORC the following:</p> <ul style="list-style-type: none"> • Can they provide a detailed diagram that shows the entire ORC architecture including ECA and SSP CAs • Where do ACEs OIDs flow into the ORC CA or do they? • Can they assert that e-Validate meets the independence requirements in the CP due to the detailed level of involvement of Brian Dilley in the CP modifications specified at the 15 March CPWG meeting? • Can they provide Mr. King with a copy of their Audit Letter? 	Matt King	April 12, 2011	May 10, 2011	Open
430	Wendy will continue interoperability testing.	Wendy Brown	April 12, 2011	June 2, 2011	Open
431	Matt King will request an Operational Review and Audit Letter from DigiCert	Matt King	April 12, 2011	May 10, 2011	Open
432	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

No.	Action Statement	POC	Start Date	Target Date	Status
433	Ms. Deb Gallagher will send digital signature guidance from ICAMSC to the Federal members of the Policy Authority	Deb Gallagher	June 14, 2011	July 12, 2011	Open
434	Matt will send request to members of the PA to research their business needs for C4CA	Matt King	June 14, 2011	July 12, 2011	Open